THE EU GENERAL DATA PROTECTION REGULATION
WHY IT MAY AFFECT YOU, AND WHAT YOU NEED TO DO

NOVEMBER 2017

INTRODUCTION

On 25 May 2018, the European Union's General Data Protection Regulation (**GDPR**) will come into force.

The GDPR will change the EU's legislative framework around how organisations collect, store and manage personal data and, as a New Zealand organisation, you may be affected by the GDPR. In this article, we discuss whether the new regulation could apply to your organisation, and what you need to do to ensure that you comply with a rapidly evolving global data protection landscape.

NEW EU DATA PROTECTION FRAMEWORK

The GDPR will introduce a number of important changes to the current EU directive, including the following:

Greater territorial scope

The GDPR applies to organisations *outside the EU* whose activities include:

1. **Offering goods or services** to EU customers/ users. Factors that determine if an organisation is caught by this include:
    - if the organisation is using the language or currency of an EU member state; and
    - if the customer/user can order goods or services from within that EU member state.
2. **Monitoring the behaviour** of EU customers/ users. This includes:
    - online tracking of the behaviour of customers/ users who are located in the EU; and
    - using cookies to profile EU customers/users and predict their personal preferences.

So any New Zealand organisation that targets EU customers and collects their personal data is likely to be subject to the obligations imposed by the GDPR. Such organisations may need to appoint a representative within the EU for compliance purposes, including to liaise locally with the relevant supervisory authority and individuals.

Accountability and compliance

Organisations that are subject to the GDPR have strict accountability obligations, including around maintaining certain documentation, conducting a data protection impact report for certain riskier types of processing, and the implementation of data protection by design and default (for example, ensuring that only personal data that is required for a particular activity is processed and retained).

In certain circumstances, organisations will need to appoint a Data Protection Officer (**DPO**). The DPO should be an individual who directly reports to the highest level of management, with sufficient knowledge of the relevant privacy regulations. The DPO can be an employee or a consultant.

The role of the DPO will be to maintain detailed records of all data processing activities and to oversee a data protection strategy ensuring that the organisation complies with the GDPR.

Consent

The GDPR will require organisations to obtain the express consent of data subjects when collecting and storing their data. This consent must be given freely, and be specific, informed and unambiguous in nature. Pre-ticked boxes will not be adequate in this regard.

Erasing personal data

The GDPR gives individuals the right to require organisations to erase their personal data without any delay. This right is accompanied by an obligation to take reasonable steps to ensure that any person who the data is disclosed is given notice of the data subject's erasure request, allowing them to comply with the request.

Requests for information

Individuals have the right to request that organisations provide them with all of the personal data that they hold.

This data must be provided by the organisation in a structured manner, and be in a commonly used format so that the personal data can be transferred to another organisation at the request of the individual.

Breaches

The GDPR places a mandatory obligation on organisations to notify the relevant supervisory body of any breaches of data that occur. Such a notification must take place without undue delay, and where feasible within 72 hours of the discovery of a breach. If this time frame is not met, then a reasoned justification must be provided. In certain cases, the affected individuals must also be informed. However, no notification is required if the breach is unlikely to result in any risk to individuals.

Fines

The fines associated with a breach of the GDPR are significant compared with the current directive. For certain higher end infringements, the organisation may be fined up to the higher of 4% of its worldwide turnover and EUR20 million.

Other lower end infringements will attract a fine of up to the higher of 2% of the organisation's annual worldwide turnover and EUR10 million. Factors such as the nature, gravity and duration of the infringement will be of relevance to the level of the fine.

TRANSFERS TO NEW ZEALAND ORGANISATIONS

Transfers of personal data to non-EU countries with an adequate level of protection do not require any specific authorisation under the GDPR. New Zealand has an adequate level of protection so transfers to New Zealand will continue to be permitted.

REFORM OF PRIVACY ACT 1993

Since the New Zealand Privacy Act was enacted in 1993, there have been significant and rapid changes in information technology and data science. This has influenced developments in international legal frameworks, culminating in the forthcoming introduction of the GDPR in May 2018.

To bring New Zealand data protection legislation in line with these new international legal frameworks, the New Zealand Government is proposing to update the Privacy Act on the back of recommendations made by the Privacy Commissioner in his recent review of the current legislation. The reform proposals include stronger powers for the Privacy Commissioner, mandatory reporting of privacy breaches, new offences and increased fines.

The Ministry of Justice, which is responsible for the proposed legislation, indicated that a Bill amending the current Act was likely to be introduced to Parliament in 2017 but it appears now that this will happen in 2018.

Clearly, until the Bill is introduced and the ensuing Act is enacted, it will be difficult for New Zealand organisations to prepare for any new legislation. However, any organisation that puts in place appropriate processes and procedures to ensure compliance with the GDPR will most likely be in a strong position from a compliance perspective when the existing New Zealand legislation is updated.

WHAT STEPS DO I NEED TO TAKE TO COMPLY?

If the GDPR applies to your organisation (and if you have not already done so), you will need to have appropriate processes and procedures in place to ensure compliance with the new legislation when it comes into force in May 2018. This will include embedding the following into your organisation:

- clear processes and procedures to address data breaches, including around notifying the relevant authorities and individuals of any breaches;
- a framework to ensure compliance with the GDPR's accountability requirements, including identifying whether a DPO will need to be appointed, and if so, appointing an appropriate DPO and providing any training that may be required;
- updating your privacy policies, including by ensuring they are written in clear and plain language, and are accessible;
- assessing how you obtain the consents of individuals, and if required, changing your processes and documentation around obtaining these consents; and
- putting in place processes and procedures to uphold individuals' rights in relation to the collection, storage and management of their personal data.

FOR MORE INFORMATION

A copy of the GDPR can be found here.

HOW WE CAN HELP

Our team of New Zealand and UK qualified lawyers would be pleased to discuss the impact of the GDPR with you in further detail, answer your questions, and assist you to comply with your obligations.

If you have any questions on the GDPR, or if you would like us to assist you to comply with its requirements, please contact one of the contributors below.

Key Jackson Russell contacts

David Alizade PARTNER
BUSINESS LAW TEAM
DDI +64 9 300 6937
M +64 21 224 8055
E david.alizade@jacksonrussell.co.nz

Claire Godber SENIOR ASSOCIATE
BUSINESS LAW TEAM
DDI +64 9 300 6916
M +64 21 425 953
E claire.godber@jacksonrussell.co.nz

Level 13 The AIG Building, 41 Shortland Street, Auckland, New Zealand
PO Box 3451 Auckland 1140, DX CP 20520

Telephone: +64 9 303 3849
Fax: +64 9 309 0902