Russell McVeagh

# Information Sheet for GDPR

May 2018

## Introduction

On 25 May 2018, the European Union's new General Data Protection Regulation ("GDPR") comes into force. Even though the GDPR is an EU regulation, it has important implications for New Zealand businesses.

We set out in the following pages some of the key considerations for you to bear in mind in determining whether the GDPR is relevant to your business and what you should be doing to get prepared.

Some GDPR terminology is slightly different to the terms used in New Zealand privacy law and we explain the meaning of these terms at the back of this note in the "Key GDPR Terms" section.

## When does the GDPR apply to New Zealand businesses?

The GDPR will apply to a New Zealand business that has an office established in the EU and that processes personal data (whether or not that processing takes place in the EU).

In addition, the GDPR also applies to New Zealand businesses that do not have an office established in the EU, but who process the personal data of data subjects residing in the EU where that processing either:

a) relates to the offering of goods or services to data subjects in the EU (irrespective of whether payment is made); or

b) relates to the monitoring of the behaviour of data subjects in the EU (e.g., through using cookies or apps to track users through multiple domains).

## What are the risks?

There are a series of potential penalties and liabilities that arise under the GDPR.

Businesses are subject to potential administrative fines. There are two tiers of penalties:

a) a fine of up to €10,000,000 or 2% of total worldwide annual turnover (whichever is highest). This fine could be imposed if, for example, a business fails to:
   - designate an EU representative;
   - report a data breach; or
   - appoint a Data Protection Officer.

b) a fine of up to €20,000,000 or 4% of total worldwide annual turnover (whichever is highest). This fine could be imposed if, for example, a business:
   - unlawfully processes personal data;
   - breaches international transfer restrictions; or
   - does not comply with an order imposed by an EU-based privacy authority.

In addition to fines, EU-based privacy authorities have a range of corrective powers and sanctions including issuing warnings and reprimands, imposing a temporary or permanent ban on data processing and ordering the rectification, restriction or erasure of data.

Fines and judgments of this nature could have serious reputational consequences for a New Zealand business, but there are some potential hurdles to EU-based authorities enforcing any such fine or judgment against an organisation with no EU presence. From a practical perspective, a more significant risk may therefore be the ability of EU-based authorities to take measures to effectively "turn off the tap" of EU data that is provided to a non-compliant business. Such action could result in serious disruption to business operations for any non-compliant overseas organisation.

## Do all business need to take the same approach?

New Zealand businesses should actively be considering the impact of the GDPR on their operations and assessing their compliance. However, different New Zealand businesses will have different levels of risk under the GDPR and, therefore, there is not a "one size fits all" approach.

A New Zealand business could be considered "high risk" if the business:

a) has an office established in the EU;

b) offers goods or services directly to EU data subjects; or

c) processes sensitive data.

A "high risk" organisation should be actively preparing for the introduction of the GDPR now. Organisations falling outside of the category of "high-risk" should be considering what steps it can implement easily now and forming an action plan as to a more staged approach to full GDPR compliance.

Whilst complying with the GDPR may require some initial investment, putting in that ground work now also presents an opportunity for businesses to form a strategy to best leverage one of their most valuable assets, their data. This will give businesses a genuine commercial advantage over their less-informed peers.

## Compared to New Zealand privacy law, what additional requirements does the GDPR contain?

The GDPR is much more prescriptive than New Zealand privacy law. There are notably stricter requirements in a number of areas of the GDPR, including the following:

| NZ PRIVACY LAW | GDPR |
|---|---|
| **Consent of data subjects to use their data for a specific purpose** | |
| can be achieved through individuals agreeing to a privacy policy | must be explicit, positively given and separate to other contractual terms – a privacy policy will not be enough |
| a business must have "reasonable grounds" to believe that they have the individual's consent | a business must receive "active consent" and has the onus of demonstrating this consent |
| **Privacy breach notification** | |
| no mandatory privacy breach notification is required (although this is proposed under the new Privacy Bill) | if a privacy breach occurs, this must be reported to the relevant privacy authority within 72 hours and, in some circumstances, reported to the affected individual as well |
| **Mandatory contractual terms in contracts with data processors** | |
| no mandatory requirements | specific mandatory clauses are required in all contracts between controllers and processors, these clauses cover:<br>- the scope of processing<br>- confidentiality<br>- security<br>- sub-processors<br>- individuals' rights<br>- storage and erasure<br>- documentation |

| NZ PRIVACY LAW | GDPR |
|---|---|
| **International transfer restrictions** | |
| personal information may be transferred outside of New Zealand at the organisation's discretion, except in very limited circumstances | personal data may only be transferred outside the EU in limited circumstances including:<br>- to countries that provide an 'adequate' level of data protection (such as New Zealand)<br>- where specific safeguards, such as standard data protection clauses or binding corporate rules, apply and on the condition that data subject's rights and remedies will remain available after the transfer<br>if personal data is transferred to New Zealand and is then on-transferred to a third party country outside of the EU, this rule also applies to any such on-transfer |
| **Accountability and governance** | |
| businesses are required to have a Privacy Officer and there are general requirements regarding security of information | businesses must demonstrate that they comply with the GDPR e.g. by:<br>- appointing a Data Protection Officer<br>- where applicable, appointing a designated EU representative<br>- carrying out risk assessments to identify, and fix, gaps in compliance<br>- keeping accurate records of collected data, its authorised uses, disclosure, and security measures<br>- training staff |
| **Rights of individuals in relation to their personal data** | |
| - the right of access to their data<br>- the right to require that their data be rectified<br>- the right to request that their data be deleted in certain circumstances | - the right of access to their data<br>- the right to require that their data be rectified<br>- the right to request that their data be deleted in certain circumstances<br>- the right to restrict processing of their data in certain circumstances<br>- the right to require that their data be transferred to another business<br>- the right to object to the processing of their data<br>- the right not to be subject to automated decision-making, including profiling |

As illustrated by the above, New Zealand businesses that comply with New Zealand's existing privacy laws cannot assume that they will automatically comply with the GDPR. In fact, most businesses will need to change their processes to become GDPR compliant.

## What can New Zealand businesses be doing now to get GDPR compliant?

The steps required to become GDPR-compliant will depend on each organisation's particular circumstances and risk level under the GDPR. However, we set out below some key changes that many organisations will need to consider. We have ordered these to range from the less onerous "low hanging fruit" which may be easier and less costly for organisations to implement, to the more onerous compliance initiatives which may require more significant investment.

1. Consider whether you collect and process personal information from data subjects residing in the EU. If so, consider the grounds upon which this is collected and processed (e.g., obtaining an individual's consent) and whether this is compliant with GDPR requirements.
2. Take steps to implement an accurate internal record-keeping system of all personal information collected and processed and the purposes for such processing.
3. Review and update privacy policies and notices to ensure that these are GDPR compliant.
4. Update your contracts with subcontractors who process personal information on the organisation's behalf to include the new mandatory clauses required by the GDPR.
5. If the organisation is itself a "data processor" that processes personal data about individuals residing in the EU on behalf of third parties, revisit contracts and standard terms and conditions with your customers to incorporate appropriate protections and mandatory clauses required by the GDPR.
6. Verify that you have the appropriate measures in place to ensure the security of the personal information held.
7. Consider how privacy by design can be introduced into the business, appoint the required representatives described above and ensure that everyone who has access to personal data receives appropriate training on the GDPR.
8. Ensure that technical and organisational measures are in place to enable compliance with individuals' rights under the GDPR with respect to their data.

## Key GDPR Terms

The GDPR uses slightly different language to the privacy laws in New Zealand. In particular, the following terms are essential when interpreting the GDPR:

- **"data subject"** – means a natural person whose personal data is processed;
- **"personal data"** – means any information related to a data subject that can be used to directly or indirectly identify the person;
- **"processing"** – has a broad definition and includes any operation performed on personal data, whether or not by automated means, including collection, use, storage, recording, etc; and
- **"sensitive data"** – means any data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or a natural person's sex life and/or sexual orientation.

## Further Information

Please get in touch with our team if you would like to discuss:


Liz Blythe
SPECIAL COUNSEL
liz.blythe@russellmcveagh.com
P +64 9 367 8145

Joe Edwards
PARTNER
joe.edwards@russellmcveagh.com
P +64 9 367 8172

Rachel O'Brien
SENIOR SOLICITOR
rachel.o'brien@russellmcveagh.com
P: +64 9 367 8880


Please see **russellmcveagh.com** for further information.