UPDATE
PRIVACY

GDPR compliance in four steps

BY **BIANCA MUELLER**

Privacy and data protection may not matter to many outside of Europe. But this will change on 25 May 2018 when new EU privacy laws will coerce global businesses with links to the continent to comply with the General Data Protection Rules (GDPR).

These new rules will impact on any international organisation handling personal data of anyone residing in the European Union.

The extraterritorial scope of the GDPR means that some New Zealand organisations and businesses need to review their internal data processing procedures, or risk hefty fines for non-compliance.

European data protection authorities will have the power to impose fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher) for any breach of the GDPR.

The GDPR can also result in civil liability. Any person who has suffered damage as a result of a breach of the GDPR has the right to receive compensation from the data controller or the data processor.

Step 1: Who needs to comply?

The GDPR is fitted with a broad territorial scope – meaning it is affecting businesses outside the EU.

EU-based entities

Any processing of personal data in the context of a branch or subsidiary in the EU must comply with the GDPR. That is the case even if the actual processing itself takes place outside the European Union.

Providers of outsourced services such as IT or admin services or cloud storage will be caught by this provision.

Example

Kiwi Ltd is offering an international money transfer service to customers worldwide. All customer data is processed and stored on a cloud storage facility hosted in the United States. Kiwi Ltd offers the service to its European customers through a German subsidiary.

Non-EU based entities processing data of individuals within the EU

All businesses with customers in the European Union or businesses that merely monitor the behaviours of individuals who live in the EU must abide by the new EU data protection standards.

These businesses must ensure that they comply with the GDPR; irrespective of their physical location. The game changer here is that even businesses without a physical presence in the EU may have to comply with the new rules if they:

- sell goods or services to a person who lives in the EU; or
- monitor the behaviour of a person who lives in the EU.

The critical factor is the location of the individual (data subject) not the location of the data processor or data controller.

Example for monitoring behaviour of EU residents

NZ Ltd (without an EU subsidiary or branch) is selling apparel online to Australian and New Zealand customers. It is considering expanding its operations to the European market. To that end, NZ Ltd uses web analytic tools to determine how many people from each European country visit the NZ Ltd website and what they are interested in.

NZ Ltd would need to comply with the GDPR because any form of web profiling or tracking, whether through cookies or otherwise, will fall into the ambit of the GDPR.

The direct consequence of this is that businesses can no longer go "forum shopping" for the lowest data protection standards in the EU.

Uncertainty exists as to how these privacy standards will be enforced in practice against an entity outside the EU, especially if they have no assets in the EU.

However, there is a reputational element at play as well. Businesses that want to succeed in the European market must therefore ensure that they comply with the GDPR.

The bigger sting may result from

Why are privacy standards high in Europe?

In Europe, the protection of persons in relation to the processing of personal data is a fundamental right.

Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

The European understanding of privacy is deeply rooted in human dignity and autonomy. It implies that each person can control and draw the line between their public and private sphere.

The basic idea is that people should be able to control personal data about them also called "informational self-determination". This means that individuals have a right to determine when, how, and for what purpose personal information about them is being held and used.

potential civil liability which would be (unlike fines) enforceable in New Zealand as a money judgment.

Step 2: What personal data is being collected and processed?

Personal data is *broadly* defined in the GDPR. Personal data is any information relating to a person *who can be identified* either directly or indirectly. Personal data may relate to a person's private, professional, or public life. It can be anything from a name, a photo, an email address, employment details, interactions on social media, medical records, or an IP address. Even a dynamic IP address can be personal data (C-582/14 2016 *Breyer v Federal Republic of Germany*). Personal data includes for instance:

- Personal details such as the person's name, address, email;
- Financial details such as how much the person earns, credit ratings;
- Medical details about a person's mental or physical health;
- Details about a person's ethnicity, political opinions, religious beliefs, or sexual life;
- Images or voice recordings of a person;
- Employment details;
- IP address of a person that visits a website;
- Criminal records or alleged offence;
- Biometric data; or
- Location data.

A person may be indirectly identifiable if identification is made possible through combining different pieces of information that by themselves alone would not reveal the identity of the person.

The GDPR does not apply to personal data that has been anonymised so that an individual can no longer be identified from the information itself. However, pseudonymised data that is retracable may be considered as personal data on individuals which are indirectly identifiable.

Step 3: How is personal data collected?

Businesses need to have a close look at how they collect personal data. Data may be collected from many sources: A person may have provided it voluntarily for "free" services such as search engine services or social networks. Personal data may also be captured automatically through cookies, web analytics, and sensors.

The GDPR approaches consent more restrictively. Consent must be "freely given, specific, informed and unambiguous". Silence, pre-ticked boxes or inactivity is not a form of valid consent.

Consent must be specific to distinct purposes for handling personal data. Consent should cover all intended processing activities.

Particular conditions are imposed in the case of children online and for sensitive personal information.

Step 4: Why is personal data processed?

Businesses need to be clear about the legal ground or grounds for which they process personal data.

The GDPR prohibits the processing of personal data unless there are legal grounds to do so. In other words just because a business *can* process personal data does not mean it is also legally entitled to do so.

- Legal grounds for processing of personal data include:
- To perform a contract;
- The individual concerned has given consent;
- The data controller has a legitimate interest;
- Statutory obligation to collect and retain information (eg, employers);
- To perform the lawful function of a public authority; or
- For the protection of vital interests of that person.

Personal data must be handled for specified and explicit purposes. During the life cycle of data, the personal data cannot be further processed in ways that are incompatible with the initial purposes for which the data was collected.

For instance, personal data that has been collected to perform a sale of goods contract cannot later be used for marketing, unless the person has specifically agreed to receiving promotional offers.

The GDPR does not provide for an intra-group privilege. Instead each group subsidiary will be accountable for its own data protection standards. This also means that intra group data transfers must be justified by law.

Example

Kiwi Holding Ltd is employing Swedish staff through its Swedish subsidiary. However, the actual payments of salaries to the Swedish staff comes from Kiwi Holding.

There is – by default – no right for the Swedish subsidiary to transfer employee data to Kiwi Holding Ltd. Express consent is required from each Swedish employee for the intra-group data transfer to be legal.

Conclusion

The GDPR has introduced extended liability and increased penalties. With this in mind, companies should be particularly careful when handling personal data of Europeans.

Businesses need to review their internal data policies and procedures that address privacy and data protection, including their IT policy, HR policy, outsourcing procedures, and any policy affecting data subjects in the European Union.

GDPR compliance is not a one-off task. It is an ongoing process. Relevant policies should therefore continuously be monitored, reviewed, and most importantly communicated to staff.

Bianca Mueller ✉ bianca@lawdownunder.com practises as a New Zealand barrister and a German lawyer. She is the founder of the technology law firm LawDownUnder which focuses on European transnational and commercial relationships with New Zealand and Australia.