PRIVACY AND DATA PROTECTION

PRIVACY AND DATA PROTECTION

Bianca Mueller
LawDownUnder
Wellington

Introduction

The sheer scale of world-wide synchronised cyber-attacks highlights that privacy and data security are one of the most pressing issues that businesses are facing today.

2017 will be remembered for Uber's massive data breach that it kept secret for over a year.[1] The data theft resulted in the unauthorised access to:

- personal information of 57 million Uber users around the world, including their names, email addresses and mobile phone numbers; and
- the names and driver's license numbers of around 600,000 drivers in the United States.

2017 will also be remembered for a new spike in ransomware attacks (a malicious form of software that uses encryption to hold data hostage until a ransom is paid).

WannaCry and Petya were massive cyber-attacks that simultaneously targeted organisations around the world, including hospitals, airlines, banks, telephone companies, railway lines, and law firms. Within 72 hours of the respective attacks, over 200,000 computers in 150 countries were affected.

New threats and the continuously changing regulatory landscape mean that an organisation's security needs are continually evolving. Practitioners will need to adjust their advice accordingly.

Dealing with cyber security attacks and privacy breaches is practically and legally challenging.

Data protection is not a one-off task. It is an ongoing process. Relevant policies and contracts should therefore continuously be monitored and reviewed.

European General Data Protection Regulation

On 25 May 2018, the European General Data Protection Regulation (GDPR) will come into effect and even though it is a European piece of legislation, it may still affect organisations here in New Zealand.

[1] Not only did Uber lose control of the private information of 57 million people, it also hid that massive breach for more than a year. At the time of the incident in 2016, Uber was negotiating with the Federal Trade Commission to settle privacy issues dating back to 2014.

The extraterritorial scope of the GDPR means that some New Zealand organisations will have to review their internal data processing procedures and adjust their privacy policies and contracts. Else they risk hefty fines for non-compliance.

Under the new law, European data protection authorities will have the power to impose fines of up to EURO 20 million or four percent of annual worldwide turnover (whichever is higher) for any breach of the GDPR.

The GDPR can also result 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 affects 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.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[2]

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.

> <u>Example 1:</u>
>
> Kiwi Limited 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 US. Kiwi Limited 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 are in the EU must abide by the new EU data protection standards.

[2] Article 4 of the GDPR.

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 interact with a person who is 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 2:
>
> Monitoring behaviour of EU residents:
>
> NZ Limited (without an EU subsidiary or branch) is selling apparel online to Australian and NZ customers. It is considering expanding its operations to the European market. To that end, NZ Limited uses web analytic tools to determine how many people from each European country visit the NZ Limited website and what they are interested in.

NZ Limited would need to comply with the GDPR because any form of web profiling or tracking, whether through cookies or otherwise, will be captured by 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 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 has a broad definition in the GDPR. It is any information relating to a person *who can be identified* either directly or indirectly. It 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.[3]

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;

[3] *Patrick Breyer v Bundesrepublik* Deutschland C-582/14 (2016).

- 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 of a person is made possible through combining different pieces of information that, by themselves, 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 (eg statistical). However, pseudonymised data that is retraceable 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".[4] Silence, pre-ticked boxes, or inactivity is not a form of valid consent.

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

More stringent conditions for consent are imposed in the case of children online[5] and for sensitive personal information.[6] As explained by Recital 38 of the GDPR children require special protection, especially online; "children may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data."

For children under 16 years of age, parental consent is required to lawfully process the personal data of children.[7]

[4] Article 7 of the GDPR.

[5] Article 8(1) of the GDPR.

[6] Article 9 of the GDPR.

[7] Article 8(2) of the GDPR.

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 may include:[8]

- 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.[9]

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 3
>
> Kiwi Holding Limited 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 Limited. 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.

[8] Article 6 (1) of the GDPR.

[9] Article 6 (4) of the GDPR.

Why are privacy standards high in Europe?

The protection of natural 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 art 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 that is about them, referred to as "right to 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.

Contracts

Adjusting Force Majeure and Hardship Clauses to account for new cyber security threats

In drafting and reviewing a contract, practitioners may wish to consider the effects of a cyber-attack on the performance of a contract. There are a number of mechanisms contracting parties can include in their contracts to deal with cyber-attacks.

Contracts are a responsibility and risk allocation task. Much depends on the context and the perceived bargaining power of the negotiating parties.

As a starting point, it may be useful to think about the following questions:

1. Would the performance of this contract be affected by a cyber-attack?
2. If yes, who should bear that risk?
    - should the contract provide for a separate provision dealing with cyber-attacks?
    - should cyber-attacks be covered in the force majeure and hardship clause?
    - does the client have a Business Continuity and Disaster Recovery Plan?
    - does the client have cyber security insurance / data breach insurance?

If the contract is silent in the event a cyber-attack occurs, then the defaulting party is left at the mercy of the common law. In this case they will have to rely on the common law doctrines of frustration and impractability.

Relying on these doctrines in the case of cyber-attacks is most likely a dead end. Cyber-attacks are hardly an unforeseeable event these days.

If the contractual performance is at risk should a cyber-attack occur, then the parties are best advised to either seek to allocated the risks contractually or to take out appropriate insurance cover.

Special risk clauses

Force majeure clauses deal with unforeseeable events that are beyond the parties control that result in an inability of one or more parties to perform their obligations under a contract (temporarily or permanently).

A force majeure triggering event must be specified in the contract such as an earthquake or power outage. Traditionally, force majeure clauses have been drafted with physical, political, and natural threats in mind:

> **Political events** such as war (military or civil), riots, acts or threats of terrorism, invasion, act of foreign enemies or embargo, rebellion, revolution, insurrection, civil disorder
>
> **Natural events** such as fire, flood, hurricane, typhoon, earthquake, lightning, draught tidal waves and floods
>
> **Labour events** lockouts, strikes or industrial action or blockade, slowdowns, prolonged shortage of energy supplies, and acts of state or governmental action
>
> **Hazardous substances** such as contamination by radio-activity from any nuclear fuel, or from any nuclear waste from the combustion of nuclear fuel, radio-active toxic explosive, or other hazardous properties of any explosive nuclear assembly or nuclear component of such assembly;

Modern force majeure and special risk clauses may also deal with cyber-attacks.

> **IT security events:** hacker attacks, denial of service attacks, ransom ware, virus or other malicious software attacks or infections.

The provision may state that in these instances the contract is temporarily suspended.

> Example 4:
>
> Either party to this Agreement may claim relief from liability for non-performance of its obligations to the extent that this is due to a Force Majeure Event.

It may also state that the contract can be terminated if the event occurs for more than a specified time.

> Example 5:
>
> Either party may, by written notice in writing, terminate this Agreement, if a Force Majeure Event lasts for a continuous period of more than 30 days.

Checklist for drafting special risk clauses concerning IT security

□ Definition of cyber-attack?

□ Notification required when a cyber-attack occurs?

□ Liability for damages, suspension, termination?

□ Service credits?

□ Duty to mitigate loss?

□ Duty to re-negotiate in good faith?

□ Who can suspend performance of contract and for how long?

□ What happens if the cyber-attack continues for more than a specified period of time? Right to terminate or (liquidated) damages?

□ Requirement to implement and comply with Business Continuity and Disaster Recovery Plan?

□ What if cyber-attack is the result of neglect or failure to take reasonable precautions (eg did not follow BCDRP, no software update, firewalls and virus software)?

□ Is Cyber Security Insurance required?

Conclusion

New threats and the continuously changing regulatory landscape mean that an organisation’s security needs are continually evolving. Practitioners will need to adjust their advice accordingly.

Businesses need to review their internal data policies and procedures that address privacy and data protection, including their IT policy, HR policy, outsourcing procedures, disaster recovery plans, and insurance policies.

When advising clients on privacy and data protection matters, practitioners will need to consider the (global) regulatory landscape, contractual aspects, and a potential need for their client to take out cyber security insurance.