officetorque

General Data Protection Regulation (GDPR) Business Guide

May 2018

LEGAL DISCLAIMER

The information contained in this guide is for general guidance purposes only. It should not be taken for, nor is it intended as, legal advice. OfficeTorque would like to stress that there is no substitute for customers making their own detailed investigations or seeking their own legal advice if they are unsure about the implications of the GDPR on their businesses. While we have made every effort to ensure that the information provided in this guide is correct and up to date, OfficeTorque makes no promises as to completeness or accuracy and the information is delivered on an “as is” basis without any warranties, express or implied. OfficeTorque will not accept any liability for errors or omissions and will not be liable for any damage (including, without limitation, damage for loss of business or loss of profits) arising in contract, tort or otherwise from the use of or reliance on this information or from any action or decisions taken as a result of using this information.

TABLE OF CONTENTS

INTRODUCTION

The General Data Protection Regulation ("GDPR") is the new legal framework that came into effect on the 25th of May 2018 in the European Union ("EU"). EU Regulations have direct effect in all EU Member States, meaning the GDPR takes precedence over any national laws.

The GDPR's focus is the protection of personal data, i.e. data about individuals. It affects not just companies but any individual, corporation, public authority, agency or other body that processes the personal data of individuals who are based in the EU. It includes your customers, employees, suppliers and any other individual you collect personal data from. Personal data includes names, contacts, medical information, credit card or bank account details and more.

GDPR gives control of personal data back to the people who own it, and it requires organisations to make data protection a core part of their operations and processes.

The GDPR has broad ranging implications for most departments within many businesses worldwide. Most businesses within the EU/UK or dealing with EU or UK entities will need to put in place additional practices and safeguards.

With the prospect of incurring fines of up to 4% of annual global turnover or 20 million Euros, whichever is the greater, knowledge of GDPR should be considered a business requirement.

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.

GDPR BASIC PRINCIPLES

The GDPR is founded on three basic sets of rules relating to personal data. In simple terms these can be outlined as follows:

Data Protection Principle

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the individual concerned. It must be collected or specified, explicit and legitimate purposes and not further processed in a way incompatible with this. Personal data collected must be adequate, relevant and limited to what's necessary. It must be accurate and kept up to date, and every reasonable step must be taken to ensure that personal data that's inaccurate is erased or rectified without delay. It must be stored in a way that identifies the individual for only so long as it's needed, and it must be processed in a way that ensures appropriate security—including protection against loss, destruction, or damage, and unauthorised or unlawful access.

Lawful Processing

Processing of personal data is only lawful if at least one of the following applies: the individual has given consent for one or more specific purposes; it's necessary for a contract to which the individual is a party, or will soon be; a legal obligation must be complied with (e.g. submission of tax records by a business); there's a task that's in the public interest or is carried out in the interest of official authority; it's necessary for legitimate interests (or those of a third party) except where overridden by the interests, fundamental rights and freedoms of the individual.

International Transfers

The GDPR continues the general prohibition on sending personal data outside the European Economic Area to a country that does not provide adequate protection. At the time of writing, the countries deemed by the European Commission to provide "adequate" protection are: US companies that self-certify to the European Union US Privacy Shield arrangement (note: this does not mean the US as a country is considered to provide adequate protection), Andorra, Argentina, Canada (limited to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay. Where no adequacy decision exists, transfers can only be made in limited circumstances, including on the basis of consent, the use of standard contractual clauses published by the European Commission or, in the case of inter-company transfers, the use of Binding Corporate Rules.

KEY CHANGES THAT YOU NEED TO KNOW

The key points of the GDPR that impact not only EU based businesses, but businesses around the world, are as follows:

Increased Territorial Scope (extraterritorial applicability)

The biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to **all** companies processing the personal data of data subjects residing in the Union, **regardless of the company's location**. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high-profile court cases. GDPR makes its applicability very clear – it applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data of EU citizens also have to appoint a representative in the EU.

Penalties

Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors – meaning 'clouds' are not exempt from GDPR enforcement.

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.

Consent

The conditions for consent have been strengthened, and companies are no longer able to use long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

DATA SUBJECT RIGHTS

Breach Notification

Under the GDPR, breach notifications are now mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors are also required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Information required to be reported:

- The data lost
- The consequences
- Counter measures undertaken

And unless the data is encrypted, you need to report the breach to the data subject whose data was lost.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability

GDPR introduces data portability – the right for a data subject to receive the personal data concerning them – which they have previously provided in a 'commonly used and machine-readable format' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically, 'The controller shall implement appropriate

technical and organisational measures in an effective way in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

DPO appointment is mandatory only for those controllers and processors of private data whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. If a DPO is required, there are internal record keeping requirements, as follows:

Importantly, the Data Protection Officer:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could result in a conflict of interest.

GDPR COMPLIANCE IN 4 STEPS

The following is an extract from an article published in Dec 2017 by the NZ Law Society which provides an overview of how to approach GDPR Compliance.

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 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 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". 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.

(Source: NZ Law Society; 01 December 2017 - By Bianca Mueller. Link to original article)

Bianca Mueller bianca@lawdownunder.com practises as a New Zealand barrister and solicitor 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.