MOSAIC™

Financial Services Infrastructure

Data Privacy

Privacy Act 2020 and GDPR

Welcome

This course comes in three main sections.

The first part of the course is the more textbook section and covers the crucial terms, legislation and regulation.

After showing you each section of the relevant regulation and legislation, this section will give a brief outline of what it means for your organisation.

The second and third part we will cover the practical and compliance side of the course, including:

- The data protection officer/ privacy officer
- Data audit
- Data security
- Data breach
- DPIA
- Step by step, guide on how to do a full data privacy implementation.
- Templates

Contents - Part one

Module one - Introduction

1. Welcome
2. Important Terms and questions
3. Understanding the basics

Module Two - Regulations

1. Data Privacy Regulation General Data Protection Regulation (GDPR)
2. Enforcements

Module Three – Legislation

1. Introduction to privacy act 2020
2. 13 information privacy principles

Module Four - Legislation

1. Notifiable Privacy Breaches
2. Assessing Harm
3. Access Directions
4. Compliance Notices
5. New offences

Privacy Act 2020

Public Act	2020 No 31
Date of assent	30 June 2020
Commencement	see section 2

Contents – Part two

Module Five – Rights and duties

1. Rights of Data subjects and individuals.
2. Duties of data controllers
3. Types of data and records

Module Six – Application of Legislation

1. Functions of the commissioner
2. Privacy officer
3. The data protection officer
4. Data audit
5. Data map
6. Information security
7. Data breach

Module Seven – Application of Legislation Part 2

1. International Transfers
2. Privacy Notice
3. Staff Training and Data protection policy
4. DPIA

Module Eight – Ten Steps to Implementation

1. Ten Steps to Implementation

Privacy Act 2020

Public Act	2020 No 31
Date of assent	30 June 2020
Commencement	see section 2

MOSAIC™ Financial Services Infrastructure

Organisation templates

1. Information security policy.
2. Data protection policy.
3. Privacy notice template.
4. GDPR roles and responsibilities.
5. DPIA template.
6. Data breach notification plan
7. Senior management support letter template.
8. Project initiation document (PID).
9. Subject access request template.

Human resources templates

1. Human resources and data protection policy
2. Social media policy.
3. Outsourcing policy.
4. Bring your device policy.
5. Confidentiality agreement
6. Consent form for unsuccessful job applicants
7. Consent form for use of data for existing employees
8. Consent to hold employee details after leaving
9. Consent form for new employees use of data

Privacy Act 2020

Public Act	2020 No 31
Date of assent	30 June 2020
Commencement	see section 2

Why is data privacy so important?

Failure to comply with the law regarding data protection can lead to severe consequences, including legal action, monetary penalties and lose goodwill and trust from clients.
A company must ensure that they do not misuse any data they have stored and also make sure no one else can.

Data Privacy is not just a tick box exercise for your company, you should also consider the broader risks to the rights and freedoms of individuals or society at large, whether it is physical, material or non-material.

Major Legislation.

In New Zealand the main piece of legislation is the privacy act 2020 which has recently came in force on December 1st 2020. We will be going through this legislation in detail latter in this course.

Organisations also need to be aware of legislation and regulations within countries that they do business for example in the UK the major regulation that we are dealing with is the European Union's General Data Protection Regulation, or GDPR.

The main piece of legislation in regards to data protection in the UK is The Data protection Act 2018, The Act focused on the regulation of the processing of information relating to individuals, to make provision in connection with the information commission's function, to make provision for a direct marketing purposes, and there are a variety of areas and elements which help to ensure that the Act achieves this goal.

California Consumer Privacy Act (CCPA)

In California, the legislation is the California Consumer Privacy Act (CCPA) and came into effect on January 1st, 2020.

The CCPA focuses almost entirely on data collection and privacy and gives Californians the right to:

1. Know what personal data is being collected about them.
2. Know whether their personal data is sold or disclosed and to whom.
3. Say no to the sale of personal data.
4. Access their personal data.
5. Request a business to delete any personal information about a consumer collected from that consumer.
6. Not be discriminated against for exercising their privacy rights.

The legislation will likely affect changes in data privacy across the whole of the U.S. rather than just in California. Suppose you are an NZ organisation and have Californians in your database or aim to have Californians customers. In that case, you will have to go by the CCPA when dealing with these customers.

Constantly changing data privacy landscape

Alongside GDPR and CCPA, The Australian government throughout 2020 is introducing the consumer data right bill, and as seen in New Zealand, the data privacy act has recently come into force.

With this constantly changing data privacy landscape and with more organisation trading and doing business internationally, it would take your organisation a long time and use up many resources trying to treat all the regulations and legislation separately.

This course will focus more on the GDPR and Privacy Act 2020.

However, the main aim of this course is to make sure your organisation information security management will have data privacy policies and information security policies that cover the fundamental principles and key individual rights that run through the majority of data privacy regulation and legislation currently in force around the Globe.

What is data protection?

Data Protection aims to make sure that all personal information regarding an individual is used, stored and transferred in the correct manner, both for privacy and for safety.
Examples of this include
Encryption, firewalls, backups, and secured servers. A data breach would be the result of insufficient data protection.

Data protection is the fair and proper use of information about people. It's part of the fundamental right to privacy – but on a more practical level, it's really about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society.

What is data privacy?

Data privacy has more to do with managing who has authorised access to the information you hold. If an individual has given you consent to store their billing information and you give this to another company to use without the individual's permission, this would be a data privacy violation. Using that same information within your own company but for another non-consenting (and therefore unauthorised) process is also a violation.

What is a data subject?

The person or persons to which a piece of data refers.
so if data contains information for example the demographics of you, then you are the data subject.

The data subject is at the centre of the GDPR.

What is the purpose?

The purpose, is why the data is being collected as defined by the Data Controller. For most companies, the purpose of collecting the data will in a very broad sense be something like: “The data is collected to provide the service that the customer pays for.” Under the GDPR personal data can only be used for the stated purpose or purposes. This means that you can’t, for example, collect the data for the provision of a service, and then sell the data to other companies without the prior knowledge or consent of the data subjects.

Care must be taken in the creation of the purpose, it must be specific and should not be too broad.

What is personal information?

Is any information relating to an identified or identifiable natural person (referred to as a data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier like a name, identification number, or location data, or to one or more factors specific to a person's physical, physiological, mental, economic, cultural, or social identity.

In the GDPR this is only regarding a living person.

This includes information like:

Name
Email address
Phone number
Banking information, credit/debit card data, purchases, loan reports
Social Insurance Number (SIN), or other identification numbers
Race, ethnic origin, religion, education or income level
Age, height, blood type, medical records.

This is a broad definition of personal data. Location data and online identifiers (including IP addresses and cookies) are new to the GDPR and we will go into more detail latter in the course.

What is sensitive personal data?

A special category of personal data, which can't be processed without express consent.

Article 9 in the GDPR defines Sensitive Personal Data as:

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Controller define by GDPR

The GDPR states the “controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”

What do they mean by processor?

Refers to any person who processes personal data on behalf of the controller. (other than a person who is an employee of the controller)

The definition can be found in GDPR Article 4.

The data processor must be able to identify the data controller for any of the data in its possession, and must upon request be able to provide information such as:

1. The identity of the data controller for the data
2. The data controller's contact information
3. The data processing purpose

Example:
Your company runs frequent direct marketing campaigns. You use a telesales company to call people who haven't bought from you recently. In this example, the telesales company and its staff who provide the service to your company would be Data Processors.

GDPR applies to both data processors and data controllers

If you are a Processor (processing the data of EU customers on behalf of a Controller)

And you are:

1. Established in the EU, even if the data processing takes place outside the EU, then GDPR applies to you.
2. Not established in the EU, but the data processing relates to offering goods or services to people in the EU, then GDPR applies to you.
3. Not established in the EU but your data processing is related to monitoring the behaviour of customers in the EU, then GDPR applies to you.

For example, an New Zealand company that offers its wine for sale in the EU is subject to GDPR. Under GDPR, companies based outside the EU that are caught by the regulation will have to appoint a representative within the EU to make sure customers have a contact point for concerns relating to their data.

They must also tell the Supervisory Authority/Regulator who their representative is.

Processor and controllers

It is really important you understand the terms processor and controller, as they set the tone for the rest of GDPR, in reference to the duties of both the controller and the processor.

In summary a controller is the company that decides how the data is processed and the Processor is a company that processes the data on behalf of the controller.

In the next Module this course is first going to look at GDPR and then is going to focus on the big changes in New Zealand legislation with the introduction of the privacy act 2020.