Module 1 – Overview of the Privacy Law

Participants successfully completing this module should be able to:

1. identify and explain the 3 key parts to the privacy requirements
2. identify the information that the Privacy Law protects
3. explain 3 related Privacy Law requirements - consent, informed consent and access to information
4. explain the importance of the privacy laws for you and your organisation.

Section 1.1 – Welcome

Provides a brief orientation to the topics covered in the module.

Section 1.2 – The Privacy Law

Explains what ‘privacy law’ means in legal terms. Introduces the three key parts to legal privacy requirements, and outlines the 10 national privacy principles.

Section 1.3 – Protected information

Examines the kind of information that is protected by privacy law. Considers the difference between ‘personal information’ and ‘sensitive information’ and obligations relating to each.

Section 1.4 – Related requirements

Introduces and looks in detail at three related privacy law requirements: consent, informed consent, and access to information.

Section 1.5 – Why comply?

Considers moral, professional and legal reasons for complying with the privacy law. Looks at the responsibilities of all employees when dealing with protected information.

Section 1.6 – Summary

Briefly restates the objectives of the module to reinforce learning.

Section 1.7 – Assessment

Provides a concise online assessment comprising multiple choice questions to evaluate participants’ understanding of key concepts of the module.
Module 2 – Collection of information

Participants successfully completing this module should be able to:

1. identify what information you can collect
2. recognise how to identify unfair ways of collecting information
3. recognise the individual’s rights when collecting information
4. explain what information is sensitive information.

Section 2.1 – Welcome

Provides a brief orientation to the topics covered in the module.

Section 2.2 – Collecting information

What is meant by collection of information? What kind of information is appropriate to collect? When is collection legally required? What is fair and reasonable collection?

Section 2.3 – Unfair collection

Explains unfair collection, including using information for purposes other than its intended purpose, misleading clients about provision, intrusive and illegal collection practices.

Section 2.4 – The individual’s rights

Outlines the rights that individuals have in relation to information collection and use, and provides best practice guidelines on correct behaviour.

Section 2.5 – Who to collect information from

Considers the difference between indirect and direct information collection, and looks at implications and moral obligations pertaining to both.

Section 2.6 – Summary

Briefly restates the objectives of the module to reinforce learning.

Section 2.7 – Assessment

Provides a concise online assessment comprising multiple choice questions to evaluate participants’ understanding of key concepts of the module.
Module 3 – Use and disclosure

Participants successfully completing this module should be able to:

1. define and give examples of 'use' and 'disclosure'
2. identify when you can use and disclose information
3. explain the use and disclosure of information for direct marketing.

Section 3.1 – Welcome

Provides a brief orientation to the topics covered in the module.

Section 3.2 – Defining use and disclosure

Explains what 'use' and 'disclosure' mean in specific terms with regard to the handling of information under privacy laws.

Section 3.3 – Disclosing information

Looks at when it is OK to use and disclose information and when it is not OK. Provides examples of ways in which information can be misused.

Section 3.4 – Direct marketing

Highlights the particular area of direct marketing and ways in which personal information may be used or misused for marketing purposes. Covers issues such as client consent, opting-out and disclosure of information to third parties for marketing.

Section 3.5 – Summary

Briefly restates the objectives of the module to reinforce learning.

Section 3.6 – Assessment

Provides a concise online assessment comprising multiple choice questions to evaluate participants' understanding of key concepts of the module.
Module 4 – Data quality and security

Participants successfully completing this module should be able to:

1. define 'data quality' and 'data security' and explain why data quality and security are important
2. identify and explain the 4 aspects of security and your role in keeping information secure
3. explain what you should do with old information - destroy or de-identify it.

Section 4.1 – Welcome

Provides a brief orientation to the topics covered in the module.

Section 4.2 – Data quality and security

Provides a precise definition of the terms ‘data quality’ and ‘data security’. Considers issues such as data reliability, accuracy, completeness and obsolescence.

Section 4.3 – Your responsibilities

Looks at four key aspects of data security that each individual should consider (physical security, computer and network security, communications security and personnel security).

Section 4.4 – Old information

What should an organisation do with information that it no longer needs? This section outlines the proper destruction and de-identification of information once it becomes obsolete.

Section 4.5 – Summary

Briefly restates the objectives of the module to reinforce learning.

Section 4.6 – Assessment

Provides a concise online assessment comprising multiple choice questions to evaluate participants' understanding of key concepts of the module.
Module 5 – Other important issues

Participants successfully completing this module should be able to:

1. explain what openness is, the client's rights and the need for a Privacy Policy Document
2. explain when access can and cannot be given, and how to correct information
3. explain the principles of identifiers, anonymity and transborder data flows.

Section 5.1 – Welcome

Provides a brief orientation to the topics covered in the module.

Section 5.2 – Openness

Outlines the three areas of the openness principle: client's rights, the privacy policy document, and transparency in your privacy practices.

Section 5.3 – Access and correction

Considers the right of individuals to access and correct information that is stored about them, including practical considerations like client identification and reasonable access charges.

Section 5.4 – Identifiers, anonymity, transborder data flows

Introduces the final three national privacy principles. Looks at what constitutes an identifier, how they may be used, clients’ rights to deal anonymously (and limitations on this right), and implications of transborder data flows.

Section 5.5 – Summary

Briefly restates the objectives of the module to reinforce learning.

Section 5.6 – Assessment

Provides a concise online assessment comprising multiple choice questions to evaluate participants’ understanding of key concepts of the module.