SYLLABUS

ICDL Arabia

ICDL Module
Data Protection

Syllabus Version 1.0

Purpose

This document details the syllabus for the Data Protection module. The syllabus describes, through learning outcomes, the knowledge and skills that a candidate for the Data Protection module should possess. The syllabus also provides the basis for the theory and practice-based test in this module.

Disclaimer

Although every care has been taken by ICDL Foundation in the preparation of this publication, no warranty is given by ICDL Foundation, as publisher, as to the completeness of the information contained within it and neither shall ICDL Foundation be responsible or liable for any errors, omissions, inaccuracies, loss or damage whatsoever arising by virtue of such information or any instructions or advice contained within this publication. Changes may be made by ICDL Foundation at its own discretion and at any time without notice.

Data Protection Module

This module sets out essential knowledge relating to data protection concepts and principles, data subject rights, the implementation of data protection policies and measures, and regulatory compliance.

Module Goals

Successful candidates will be able to:

- Understand concepts relating to personal data and its protection.
- Understand the rationale, objectives, and scope of the European Union General Data Protection Regulation (GDPR).
- Outline the key principles of the GDPR relating to the lawful processing of personal data.
- Understand the rights of data subjects and how they are upheld.
- Understand that company policies and methods should comply with data protection regulations, and outline key technical and organisational measures to achieve this.
- Understand how to respond to data breaches and the consequences of not complying with data protection regulations.

CATEGORY	SKILL SET	REF.	TASK ITEM
1 Concepts	*1.1 Personal Data*	1.1.1	Understand the term privacy and its associated rights. Be aware that privacy is not an absolute right and other rights may take precedence.
		1.1.2	Define the term personal data.
		1.1.3	Understand the term data processing.
		1.1.4	Distinguish between automated and manual data processing.
	1.2 Protecting Personal Data	1.2.1	Understand the term data protection.
		1.2.2	Recognise some risks to personal data from data processing like: accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access.
		1.2.3	Recognise some risks for data subjects from personal data processing like: discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality, loss of privacy, loss of rights, loss of data control, profiling.
		1.2.4	Understand data protection roles and responsibilities like: data subject, data processor, data controller, data protection officer (DPO), supervisory authority.
2 GDPR Overview	*2.1 Rationale and Objectives*	2.1.1	Understand that the General Data Protection Regulation (GDPR) is a data protection regulation that is enforceable as law in all European Economic Area (EEA) member states.

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.1.2	Recognise the rationale for the introduction of the GDPR: increased legal certainty, increased consumer confidence and trust, increased protection of growing volumes of electronic personal data and their international transfer.
		2.1.3	Outline the primary objectives of the General Data Protection Regulation: equivalent level of protection of natural persons with regard to the processing of personal data, free flow of personal data throughout the European Union (EU).
	2.2 Scope	2.2.1	Outline the scope of data processing activities covered by the GDPR: automated and manual processing of personal data, personal data processing activities exempted from the application of the regulation.
		2.2.2	Outline the territorial scope of the GDPR regarding the location of personal data processing and data subjects.
3 Principles	*3.1 Processing Personal Data*	3.1.1	Define the principle of lawfulness, fairness and transparency.
		3.1.2	Define the principle of purpose limitation.
		3.1.3	Define the principle of data minimisation.
		3.1.4	Define the principle of accuracy.
		3.1.5	Define the principle of storage limitation.
		3.1.6	Define the principle of integrity and confidentiality.
		3.1.7	Define the principle of accountability.
	3.2 Lawfulness of Processing	3.2.1	Outline the conditions under which personal data processing is lawful: consent by data subject, performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest, pursuance of legitimate interests by the controller or by a third party.
		3.2.2	Be aware that consent can only be considered given by the data subject if certain conditions are met. Outline the conditions for consent: recorded, clearly requested, withdrawable, given freely.
		3.2.3	Understand the conditions applicable to a child's consent in relation to online services.

CATEGORY	SKILL SET	REF.	TASK ITEM
		3.2.4	Recognise that where processing is carried out on behalf of a data controller, a legal agreement must be in place between the data controller and data processor that ensures compliance with data protection regulations and protects the rights of data subjects.
		3.2.5	Identify special categories of personal data that are typically prohibited from processing: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric information, health, sex life, sexual orientation. Recognise that special categories of data can be processed lawfully under certain conditions like explicit consent.
		3.2.6	Recognise that in general personal data can only be transferred outside the EU for processing when the external data protection regulations are compliant with the GDPR.
4 Data Subject Rights	*4.1 Facilitate Rights*	4.1.1	Recognise the importance of clearly communicating to the data subject information relating to processing like: privacy notice, fair processing notice.
		4.1.2	Outline key information that must be provided to a data subject when personal data is obtained like: the data controller's identity and contact details, the purpose and legal basis of processing, the data retention period, the data subject's rights.
		4.1.3	Outline additional information that may need to be provided to a data subject when personal data is obtained by the data controller like: data transfer to a third country, contact details for any DPO, any other recipients, any other information to make the processing fair.
		4.1.4	Be aware that additional information should be provided to the data subject when data is not obtained directly by the data controller.
	4.2 Exercise Rights	4.2.1	Define the term subject access request and understand a data subject's right of access.
		4.2.2	Understand the right to rectification.
		4.2.3	Understand the right to be forgotten.
		4.2.4	Understand the right to restriction of processing.
		4.2.5	Understand the right to data portability.
		4.2.6	Understand the right to object and not to be subject to a decision based solely on automated processing, including profiling.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.2.7	Understand that the rights of the data subject may not be met if there are legal restrictions.
5 Implementation	*5.1 Policies and Methods*	5.1.1	Understand that organisational data protection guidelines and policies must be compliant with data protection regulations. Be aware of the importance of adhering to organisational data protection guidelines and policies.
		5.1.2	Understand that data processing should incorporate data protection by design and by default.
		5.1.3	Understand the term data protection impact assessment and when it is required.
	5.2 Measures	5.2.1	Recognise some appropriate technical and organisational measures to manage risks when processing personal data like: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services; the ability to restore personal data in a timely manner; a process for determining the effectiveness of technical and organisational measures.
		5.2.2	Be aware of specific technical measures to manage risks when processing personal data like: encryption, secure digital storage, back up data, secure digital communications, secure physical environment, secure disposal of data.
		5.2.3	Be aware of specific organisational measures to manage risks when processing personal data like: training, processes and procedures, legal contracts, managerial oversight.
		5.2.4	Distinguish between the pseudonymisation and anonymisation of personal data.
6 Compliance	*6.1 Data Breaches*	6.1.1	Understand the term personal data breach.
		6.1.2	Be aware when the data controller must report personal data breaches to the supervisory authority. Be aware of the associated time frame for reporting.
		6.1.3	Be aware that the data controller should report personal data breaches to the data subject when there is a high risk to their rights and freedoms.
	6.2 Enforcement	6.2.1	Identify the supervisory authority in your jurisdiction and recognise the requirement to cooperate with it when requested.
		6.2.2	Be aware of the data subject's right to lodge a complaint to their supervisory authority, regardless of where their data is processed.

CATEGORY	SKILL SET	REF.	TASK ITEM
		6.2.3	Understand possible consequences for organisations that fail to implement relevant data protection regulations like: fines, litigation, reputational damage.