# Practitioner Certificate in Data Protection (GDPR)

## Distance Learning Programme Syllabus

The Syllabus for the **Practitioner Certificate in Data Protection Programme (Distance Learning)** covers all practical aspects of European data protection law and practice.

Candidates study the General Data Protection Regulation (GDPR), as well as relevant decisions of the Court of Justice of the European Union and key guidance from the European Data Protection Board and supervisory authorities.

Completion of the Programme, including passing the Examination, demonstrates that the candidate has achieved a thorough understanding of the practical application of EU data protection law and practice.

The Syllabus comprises 14 Learning Modules:

1. Introduction and Territorial Scope
2. Terminology and Definitions
3. The Rules of Data Protection
4. Accountability and Transparency
5. The Six Lawful Justifications for Data Processing
6. Special Category Personal Data
7. Rights of Individuals
8. Data Security
9. Notifying Security Breaches
10. Outsourcing
11. Role of the Data Protection Officer
12. Data Protection Impact Assessments
13. International Data Transfers
14. Enforcement by Supervisory Authorities

Upon completion of the Programme, candidates will understand:

- when and how data protection law applies to organisations, including extra territorial applicability of the GDPR globally
- all key definitions, including 'personal data', 'data subject', 'controller', 'joint controllers', 'processor', 'consent', 'profiling', 'genetic data', 'biometric data', 'pseudonymisation', 'personal data breach', 'special category personal data', 'data protection by design', 'data protection by default'
- the distinction between electronic and manual records
- accountability and transparency – what these concepts mean and how to ensurecompliance within the organisation
- the six conditions that allow the processing of personal data
- the requirements for using 'special categories' of personal data (such as information on health, political opinions and sexual life), as well as information on criminal convictions
- the special rules that apply to holding and using data on children
- data retention – the restrictions on keeping data, and how to establish a retention schedule
- data quantity – the rules on how much data may be collected for specific purposes
- the right of subject access, including analyzing requests, collating data, applying exemptions, removing third party data, redacting documents and responding to requests
- the other rights of individuals – automated decisions, data deletion, data portability, profiling, the right to object to processing, the right to restriction of processing
- transferring data to third parties – the legal requirements for transferring data between organisations, including responding to requests for personal data from persons other than the data subject
- the exemptions – how the exemptions operate and when they are available
- data security, including encryption and pseudonymisation, data protection by design, data protection by default, the requirements for using external contractors, staff training
- data breach notifications – when security breaches must be notified to the national supervisory authority, and when they must be notified to data subjects

- international data transfers - the restriction on sending personal data outside the European Economic Area, including the distinction between 'safe' and 'non-safe' countries, the relevance of adequacy decisions, the derogations and exemptions (including consent, contractual necessity, 'model contracts', and binding corporate rules), determining the most practical and cost effective method to achieve data export goals, solutions for using foreign service providers such as offshore call centres or IT outsourcing suppliers
- the legal requirements for outsourcing personal data processing operations (using 'processors' and 'sub-processors')
- data protection impact assessments (DPIAs) – when and how to carry out an assessment, including understanding the nature and types of DPIAs, determining when a DPIA should be carried out, methodology for conducting DPIAs
- data destruction – methods to ensure lawful and secure destruction
- the role of the Data Protection Officer
- the role of the national regulators – compliance and enforcement, including powers of investigation and the imposition of fines on organisations