Practitioner Certificate in Data Protection (PC.dp.)

Syllabus

The Syllabus for the Practitioner Certificate in Data Protection Programme covers all practical aspects of data protection law and practice.. Completion of the Programme, including passing the Examination, demonstrates that the candidate has achieved a thorough understanding of the practical application of data protection legal requirements.

Part 1 of the Syllabus (80% of the total), the Core Elements, is composed of three sections:

- Fundamentals
- Access Requests
- Data Security and Cybersecurity

Part 2 of the Syllabus (20% of the total), the Elective Element, allows candidates to choose one of the following subject areas:

- Data Protection in the Workplace
- International Data Transfers
- Conducting Data Protection Impact Assessments

The content of each of the elements of the Syllabus is set out below, including percentages showing the proportion of the whole syllabus attributed to the specific elements.

Part 1

Fundamentals (40%)

- when and how data protection law applies to organisations, including extra territorial applicability under the GDPR
- the main definitions, including 'personal data', 'special category personal data', 'data subject', 'controller', 'processor', 'consent', 'profiling', 'pseudonymisation', 'personal data breach'
- the distinction between electronic and manual records
- the requirement for transparency – what to include in, and how to draft, data privacy notices
- the requirement for fair and transparent processing
- the requirements for using 'special categories' of personal data
- data retention – the restrictions on keeping data, and how to establish a retention schedule
- individuals' rights – subject access, 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 main exemptions – an understanding of how the exemptions operate and when they are available
- the legal requirements for gathering information for marketing, including the distinction between, and the drafting of, opt-out and opt-in clauses
- how the choice of media (email, text message, fax, telephone, post) affects the conduct of the marketing campaign
- the implications of using cookies and other tracking technologies on websites
- an introduction to the restriction on cross border data transfers and the possible methods for legitimising data exports
- the legal requirements for outsourcing personal data processing operations (using 'processors' and the engagement of 'sub-processors')
- data destruction – methods to ensure lawful and secure destruction
- an introduction to data protection impact assessments – the basics of when and how to carry out an assessment
- accountability – the requirement for, and necessary content of, data protection policies
- the role of the Data Protection Officer
- the role of the national data protection regulator – compliance and enforcement, including powers of investigation and the imposition of fines on organisations

Access Requests (20%)

- determining whether a valid request has been made for access
- liaising with the applicant to clarify the request, if needed
- relevant time limits, including pausing the clock to clarify requests
- analysing whether any manual (paper) records fall within the request
- setting parameters for the search for information and collating the results
- establishing whether the retrieved information is personal data
- understanding what amounts to a 'reasonable and proportionate' search
- dealing with third party information, including handling redaction operations
- applying relevant exemptions
- presenting the response to the requester
- managing dissatisfied requesters
- the role of the data protection regulator
- ensuring appropriate staff awareness and training
- establishing a policy/procedure for handling subject access requests

Data Security (20%)

- detailed analysis of the legal requirements for ensuring the security of personal data
- cybersecurity fundamentals
- applicable regulatory regimes including guidance from regulators
- data security implications of using external contractors and outsourced service providers, including the necessary pre-contract checks and the content of contracts
- introduction to 'privacy-by-design' and 'privacy-by-default'
- appropriate rules for managing portable electronic devices
- staff vetting, testing and training

- notification of security breaches: understanding when it is a legal requirement to notify the data protection regulator and/or affected individuals
- managing a data security breach – law and best practice
- confinement strategies

Part 2

Candidates must choose one of the following three Elective Elements (20% each)

Data Protection in the Workplace ('the Staff Data Elective')

- obtaining, using and managing staff information
- ensuring that the recruitment and selection process meets the legal requirements, including the content of application forms, pre-employment vetting, criminal records, medical checks and the interview process
- retaining staff records, including setting appropriate periods of time for keeping information
- dealing with information requests from staff
- disclosing staff information to external third parties
- references and the rights of ex-members of staff
- monitoring staff activities and communications, including using private detectives, CCTV cameras, email monitoring
- monitoring and website monitoring technologies
- handling relevant 'special category' information such as health and sickness records and medical data
- how to handle mergers, acquisitions and restructuring
- outsourcing functions to third party providers
- relevant national regulator guidance

International Data Transfers ('the International Elective')

- analysis of the restrictions on transferring (or making available) personal data abroad, including what amounts to a 'transfer'
- consideration of the distinction between 'safe' and 'non-safe' countries
- detailed consideration of 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

Conducting Data Protection Impact Assessments ('the DPIA Elective')

- understanding the nature and types of DPIAs
- determining when a DPIA should be carried out
- methodology for conducting DPIAs
- guidance from national regulators
- reviewing DPIAs