Practitioner Certificate in Data Protection

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
- Subject Access Requests
- Data Security

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

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
- the main definitions – 'personal data', 'data subject', 'data controller', 'data processor'
- the requirements for using 'sensitive personal data'
- individuals' rights – subject access, cessation of direct marketing, automated decisions
- data retention – the restrictions on keeping data, and how to establish a retention schedule
- 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 – crime and tax, disclosures required by law and legal professional privilege – and the distinction between the 'subject information provisions' and the 'non-disclosure provisions'
- criminal offences – an introduction to the main offences, including potential penalties
- what types of communication constitute 'marketing'
- how the choice of media (email, text message, fax, telephone, post) affects the conduct of the marketing campaign
- the distinction between targeting corporate entities and individuals for marketing purposes
- the purpose and effect of opt-out and opt-in clauses, including how to draft such clauses to achieve desired outcomes
- analysis of the exemption from the opt-in requirement for email marketing campaigns
- 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 'data processors' and the engagement of 'sub-processors')

- the role of the Data Protection Commissioner – compliance and enforcement, including powers of the Commissioner
- data destruction – methods to ensure lawful and secure destruction
- privacy impact assessments – the basics of when and how to carry out an assessment
- accountability – an introduction to the meaning of accountability

Subject Access Requests (20%)

- determining whether a valid request has been made for subject access
- liaising with the applicant to clarify the request
- time limits and fees
- 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
- dealing with third party information, including applying the reasonableness test and handling redaction operations
- applying relevant exemptions, including crime and taxation, back-up data, adoption records and research and statistics
- the operation of the 'disproportionate effort' exemption from the requirement to supply data in permanent form
- presenting the response to the applicant
- managing dissatisfied recipients
- the role of the Data Protection Commissioner
- 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
- applicable regulatory regimes including guidance from regulators
- data security implications of using external contractors and outsourced service providers
- information security standards, including ISO27001
- encryption of portable electronic devices
- staff vetting and testing
- staff training
- security breaches: informing individuals and the Office of the Data Protection Commissioner
- managing a data security breach – law and best practice
- confinement strategies

Part 2

Candidates must choose <u>one</u> of the following two 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 and website monitoring technologies
- handling relevant sensitive information such as health and sickness records and medical data
- how to handle mergers, acquisitions and restructuring
- outsourcing functions to third party providers
- relevant guidance from the Data Protection Commissioner

Transferring Data Abroad ('the International Elective')

- analysis of the restrictions on sending personal data outside the European Economic Area 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', binding corporate rules and 'safe harbor'
- determining the most practical and cost effective method to achieve data export goals
- security implications of using foreign service providers such as offshore call centres or IT outsourcing suppliers