BCS Practitioner Certificate in Data Protection 2017 Syllabus

Version 8.6
April 2019

This professional certification is not regulated by the following United Kingdom Regulators - Ofqual, Qualifications in Wales, CCEA or SQA

BCS GDPR Update: Practitioner Certificate in Data Protection 2017

Contents

Introduction 4
Objectives 4
Course Format and Duration 5
Eligibility for the Examination 5
Format of the Examination 5
Additional Time 5
For candidates requiring reasonable adjustments 5
For candidates whose language is not the language of the examination 5
Use of Calculators 6
Syllabus 7
1 Context (2 Hours, 5%, K3) 7
2 GDPR and Data Protection Act definitions and terminology (1.5 hours, 3.75%, K3) 8
3 Structure of the UK Data Protection Act 2018 in relation to the GDPR (0.5 hours, 1.25%, K2) 9
4 The role of the ICO as the UK Supervisory Authority (0.5 hours, 1.25%, K2) 9
5 Enforcement (including roles of the first-tier tribunal and the courts) (0.5 hours, 1.25%, K2) 10
6 Notification and record keeping obligations (0.5 hours, 1.25%, K2) 10
7 The data protection principles (4 hours, 10%, K3) 10
8 Lawfulness of processing – how to comply (4 hours, 10%, K3) 11
9 Individual rights (3 hours, 7.5%, K3) 11
10 Restriction on data subject rights (3 hours, 7.5%, K3) 12
11 Offences (0.5 hours, 1.25%, K2) 13
12 Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003 (1 hour, 2.50%, K2) 13
13 Other associated legislation (1 hour, 2.50%, K2) 14
14 Application of data protection legislation (18 hours, 45%, K3) 14
Levels of knowledge / SFIA levels 16
Format of Examination 17
Trainer Criteria 17
Classroom size 17
Recommended Reading List 18

Change History

Any changes made to the syllabus shall be clearly documented with a change history log. This shall include the latest version number, date of the amendment and changes made. The purpose is to identify quickly what changes have been made.

Version Number	Changes Made
V 8.6 April 2019	Renamed Data Protection 2018 for clarity. Amended all refs of DP Bill to DP Act. Numbering of learning objectives amended.
V 8.5 December 2017	Corrected typo and numbering. Added revision date to title.
V 8.4 December 2017	Wording change in Section 6 to correctly reflect upcoming changes in legislation (May 2018)
V 8.3 December 2017	Corrected formatting
V 8.2 December 2017	Add marking scheme to Format of Examination Table
V 8.1 November 2017	Amends to wording in section 7
V 8.0 November 2017	Syllabus amended in line with GDPR and Data Protection Bill
V7.4 December 2016	Strapline regarding regulated statement has been added
V7.3 March 2015	Updated language requirements for extra time and use of dictionaries and the broken hyperlinks. Standardised the trainer requirements
V7.2 October 2013	Trainer requirements updated
V7.1 September 2012	Added Reasonable Adjustments section and updated trainer requirements details and included a section to cover excerpts from BCS books
V7.0 May 2012	ISEB replaced with BCS. No change to content of syllabus
V6.2 June 2011	Added in Recommended Reading and Resource List
V6.1 May 2011	Additions: Warrants (entry/inspection) (2.1.2.1) ICO new enforcement powers (2.1.2.1) including s55 (3A)

Introduction

Knowledge of UK data protection law, and an understanding of how it is applied in practice, is important for any organisation holding personal data. The BCS Practitioner Certificate in Data Protection 2017 is designed for those with some data protection responsibilities in an organisation or who, for other reasons, wish to achieve and demonstrate a broad understanding of the law, including the EU General Data Protection Regulation (GDPR), the UK Data Protection Act 2018 and their practical application. It is recognised that those with overall responsibility for data protection within an organisation will need to develop a detailed understanding of the law, including those provisions which are not covered in the syllabus.

Objectives

The BCS Practitioner Certificate in Data Protection 2017 is intended to promote an understanding of the practical application of UK data protection law, including placing it in a human rights context. By obtaining the certificate, candidates will:

- Hold a recognised qualification in data protection
- Gain an understanding of the key changes and the associated implications that the GDPR and the UK Data Protection Act 2018 introduce to data protection
- Gain an understanding of individual and organisational responsibilities under the GDPR and the new UK Data Protection Act, particularly the need for effective record keeping
- Be able to apply the new rights available to data subjects and understand the implications of those rights
- Be able to demonstrate an understanding of the designation, position and role/ tasks of a data protection officer
- Be able to prepare organisations to manage and handle personal data in compliance with the GDPR and the UK Data Protection Act 2018.

Target Audience

This qualification is aimed at those candidates who have, or wish to have, some responsibility for data protection within an organisation and need to understand the changes that the GDPR and the UK Data Protection Act 2018 bring to data protection legislation, including what needs to be done to prepare their organisations for compliance. The certificate will also be useful for others who wish to obtain and demonstrate a broad understanding and application of the UK's data protection regime. It is ideal for those candidates who already hold the Foundation Certification in Data Protection and who want to gain a more in-depth knowledge of interpreting and applying the principles of data protection legislation and the GDPR in particular.

Course Format and Duration

Candidates can study for this certificate in two ways: by attending an accredited training course or by self-study. An accredited training course will require a minimum of 40 hours of study run over a minimum of five days. The course can be delivered in a number of different ways from traditional classroom-based training to online e-learning.

Eligibility for the Examination

There are no mandatory requirements for candidates taking the examination, although candidates will need a good standard of written English. This is a practitioner level qualification and draws upon various legislation and directives (including the GDPR); candidates will be required to demonstrate the ability to apply the principles and requirements in a work context. Candidates are strongly recommended to complete an accredited training course. It is also recommended that candidates prepare for the course and examination by committing to personal study before and during the course.

Format of the Examination

- 120 minute 'closed book'
- 20 simple multiple-choice questions and 20 complex multiple-choice questions
- 12 short answer written questions
- Pass mark is 78/120 (65%)
- Distinction mark is 96/120 (80%)

Additional Time

For candidates requiring reasonable adjustments

Please refer to the reasonable adjustments policy for detailed information on how and when to apply.

For candidates whose language is not the language of the examination

If the examination is taken in a language that is not the candidate's native/official language, candidates are entitled to:

- 25% extra time
- Use their own **paper** language dictionary (whose purpose is translation between the examination language and another national language) during the examination. Electronic versions of dictionaries will **not** be allowed into the examination room.

Guidelines for Accredited Training Providers

It is required that all courses accredited for the BCS Practitioner Certificate in Data Protection 2017 will provide a minimum of 40 study hours.

Each major subject heading in this syllabus is assigned an allocated time. The purpose of this is two-fold: first, to give both guidance on the relative proportion of time to be allocated to each section of an accredited course and an approximate minimum time for the teaching of each section; second, to guide the proportion of questions in the exam. Accredited Training Providers may spend more time than is indicated and candidates may spend more time again in reading and research. Courses do not have to follow the same order as the syllabus. Courses may be run as a single module or broken down into two or three smaller modules.

Note that specific laws and legal issues relating to the country(ies) within which a training provider operates may be mentioned as examples and included in course material, but the examination will only test the principles.

This syllabus is structured into sections relating to major subject headings and numbered with a single digit section number. Each section is allocated a minimum contact time for presentation.

Use of Calculators

No calculators or mobile technology will be allowed.

Syllabus

For each top-level area of the syllabus a percentage and K level is identified. The percentage is the exam coverage of that area, and K level is the maximum level of knowledge that may be examined for that area.

1 Context (2 Hours, 5%, K3)

This topic ensures the candidate can summarise the evolution of data protection law in the UK and the relationship with the EU General Data Protection Regulation (GDPR). The syllabus reflects the legal provisions of the new UK Data Protection Act 2018, as well as reflecting the role of the Information Commissioner's Office (ICO), the UK's Supervisory Authority.

1.1 Privacy: The candidate will be able to demonstrate an understanding of an individual's right to private and family life and will be able to explain the relevance of confidentiality and respect for home and family life and correspondence.

1.2 History of data protection legislation in the UK: The candidate will be expected to describe the history of data protection in relation to the European Convention for the Protection of Human Rights and Fundamental Freedoms and will be able to explain the rights to freedom of expression, including:

- 1.2.1 European Convention of Human Rights and Fundamental Freedoms (ECHR), Article 8 – Respect for privacy and family life
- 1.2.2 Council of Europe Convention 108, 1981, its implementation by the Data Protection Act 1984, and updating of Convention 108
- 1.2.3 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013
- 1.2.4 Data Protection Directive 95/46/EC
- 1.2.5 Human Rights Act 1998
- 1.2.6 Telecommunications Directive 97/66/EC, Privacy and Electronic Communications
- 1.2.7 Directive 20002/58/EC, and subsequent revisions of the latter
- 1.2.8 The need for the General Data Protection Regulation 2016/679
- 1.2.9 UK Data Protection Act 2018 (implementing the GDPR in the UK)
- 1.2.10 EU Directive 2016/680 The Law Enforcement Directive (LED)
- 1.2.11 UK's Freedom of Information Act and Freedom of Information (Scotland Act) and the ability to access any recorded personal information held by a public body)
- 1.2.12 Telecommunications Directive 97/66/EC, Privacy and Electronic Communications Directive 20002/58/EC, and anticipated revisions (ePrivacy Regulation 2017/0003 (COD)

NB: Candidates are not expected to have a detailed knowledge of the content of the above, or the chronological order but should be able to explain the relationship between them and how data protection rights have evolved as a result**.**

1.3 Territorial scope and jurisdiction of the GDPR: The candidate will be able to describe how the wider scope of the GDPR impacts the processing of personal data by global organisations, and those who may not have a business (legal entity) established within the EU, including:

1.3.1 The concept of main establishment and the implications for global organisations, including the enterprise and group of undertakings (concept of one stop shop)
1.3.2 Co-operation between supervisory data protection authorities
1.3.3 When a representative of the data controller is needed

1.4 General principles for transfers of personal data to third countries: The candidate will be able to describe the measures required under the GDPR to safeguard the rights and freedoms of individuals when personal data is transferred outside of the EU, including:

1.4.1 General principles for transfers
1.4.2 Transfers on the basis of an adequacy decision by the EU
1.4.3 Transfers subject to appropriate safeguards
1.4.4 Binding Corporate Rules
1.4.5 Exemptions for specific situations

2 GDPR and Data Protection Act definitions and terminology (1.5 hours, 3.75%, K3)

2.1 The candidate is able to interpret the major definitions in the GDPR and the Data Protection Act.
2.2 The candidate is also able to explain these definitions and identify what information and processing activities are subject to the GDPR. The major definitions to be included are as follows:

2.2.1 Personal data
2.2.2 Special category personal data
2.2.3 Processing
2.2.4 Data controller, joint data controllers
2.2.5 Data processor
2.2.6 Public authority, Scottish public authority and public body, (including Crown and Parliament)
2.2.7 Manual unstructured data held by a FOIA/FOISA public authority
2.2.8 Filing system
2.2.9 Recipient
2.2.10 Third party
2.2.11 Profiling
2.2.12 Pseudonymisation
2.2.13 Consent
2.2.14 Child's consent in relation to information society services
2.2.15 Personal data breach
2.2.16 Derogations and recitals
2.2.17 Purely personal or household purposes
2.2.18 The special purposes

NB: The candidate will also be able to describe why the special purposes set out in the Data Protection Act (Schedule 2, Part 5) provide for an appropriate balance between freedom of expression and privacy.

3 Structure of the UK Data Protection Act 2018 in relation to the GDPR (0.5 hours, 1.25%, K2)

3.1 The candidate will be able to understand and explain the high-level structure of the Data Protection Act 2018, to include:

- 3.1.1 The Data Protection Act 2018 structure
- 3.1.2 Part 1 – Preliminary Overview and Terminology
- 3.1.3 Part 2 – General Processing
- 3.1.4 Part 2, Chapter 1 – Scope and Definitions
- 3.1.5 Part 2, Chapter 2 – The GDPR
- 3.1.6 Part 2, Chapter 3 – Other General Processing
- 3.1.7 Part 3, Law Enforcement Processing
- 3.1.8 Part 4, Intelligence Services Processing
- 3.1.9 Part 5, The Information Commissioner
- 3.1.10 Part 6, Enforcement
- 3.1.11 Part 7, Supplementary Provisions
- 3.1.12 Schedules 1 to 18

3.2 The candidate is also able to identify where the GDPR is adopted within that structure and demonstrate the importance of Part 2, Chapters 1 to 3.

4 The role of the ICO as the UK Supervisory Authority (0.5 hours, 1.25%, K2)

4.1 The candidate will be able to describe the role and general powers and obligations of the UK Information Commissioner's Office (ICO) as the UK Supervisory Authority, including co-operation between Supervisory Authorities, the role of the European Data Protection Board (EDPB).

- 4.1.1 Monitoring and enforcement
- 4.1.2 Promotion of public awareness and understanding
- 4.1.3 Promotion of awareness to controllers and processors of their obligations
  - 4.1.3.1 Promotion or production of Codes of Practice
- 4.1.4 Promotion of approved privacy seals, certification schemes and availability of commonly used standards (including BS 10012:2017)
- 4.1.5 Providing information to data subjects on the exercise of their rights and co-operate with the LED and another supervisory authority to provide such information
- 4.1.6 Co-operation with the LED and other data protection Supervisory Authorities including provision of mutual assistance
- 4.1.7 Conducting investigations on the application of the GDPR and LED on behalf of a supervisory authority from another state
- 4.1.8 Monitoring developments in relation to information and communications technologies and contribute to the activities of the EDPB
- 4.1.9 Advice and reporting to Parliament, the UK Government and other bodies
- 4.1.10 Dispute resolution between Supervisory Authorities by the EDPB

5 Enforcement (including roles of the first-tier tribunal and the courts) (0.5 hours, 1.25%, K2)

5.1 The candidate will be able to describe the following supervisory functions and powers:

- 5.1.1 Requests for assessments, Assessment Notices and carrying out assessments
- 5.1.2 When the ICO can issue an information notice
- 5.1.3 How the ICO uses 'undertakings'
- 5.1.4 When the ICO can issue an Enforcement notice
- 5.1.5 When and who can prosecute offences under the DPA
- 5.1.6 When the ICO can serve a monetary penalty
- 5.1.7 The role of appeals and tribunals

6 Notification and record keeping obligations (0.5 hours, 1.25%, K2)

6.1 The candidate will be able to explain circumstances of notification to the Commissioner, including:

- 6.1.1 Notification under the Data Protection Act 2018
- 6.1.2 Exemptions from notification under the Data Protection Act 2018
- 6.1.3 The impact of Section 108 of the Digital Economy Act 2017 on UK notification
- 6.1.4 The UK notification scheme replacement
- 6.1.5 Record keeping requirements of controllers and processors (Article 30)
- 6.1.6 Record keeping with respect to the Accountability Principle

7 The data protection principles (4 hours, 10%, K3)

7.1 The candidate will be able to demonstrate how the six GDPR principles set out in Article 5(1) regulate the processing of personal data and how they are enforced.

7.2 The candidate will be able to describe the data controller and data processor accountability established in Article 5(2).

7.3 The candidate will also be able to explain how each principle applies to the processing of personal data, and demonstrate an understanding of the need to interpret and apply the principles in practice, including:

- 7.3.1 The application of the right to be informed (transparency) and assessment of compatibility of further processing as part of Principle 1 of the GDPR
- 7.3.2 The link to GDPR Article 6 (4 c) and in the case of special category personal data the link to Article 9 and 10
- 7.3.3 The practical requirements that are a consequence of compliance with each Principle in Article 5 (1)
- 7.3.4 The obligations to demonstrate the accountability principle established in Article 5 (2)

8 Lawfulness of processing – how to comply (4 hours, 10%, K3)

8.1 The candidate will be able to select and apply the lawful conditions (grounds) that must be satisfied in order to legitimise the processing of personal data, including:

- 8.1.1 Consideration of the GDPR's Article 6 grounds for processing personal data and Article 9 grounds for processing special categories of personal data
- 8.1.2 Conditions for consent (transparency, communication and modalities; recitals 32 and 42 are included)
- 8.1.3 Information to be provided where personal data is obtained from the data subject
- 8.1.4 Information to be provided where personal data has not been obtained from the data subject
- 8.1.5 Consent in the context of a child's personal data, specifically in relation to information society services (to include children in Scotland)
- 8.1.6 Data minimisation and pseudonymisation (role in Data Protection by design)
- 8.1.7 Processing:
  - 8.1.7.1 Relating to criminal convictions and offences
  - 8.1.7.2 Which does not require identification
  - 8.1.7.3 Using national identifiers
  - 8.1.7.4 In the context of employment
  - 8.1.7.5 In relation to obligations of professional secrecy and duty of confidentiality under the law
  - 8.1.7.6 For the purpose of archiving in the public interest, scientific or historical research or statistical purposes

9 Individual rights (3 hours, 7.5%, K3)

9.1 The candidate will be able to demonstrate how rights and freedoms of data subjects conferred by the Data Protection Act 2018 can be applied and enforced. Specifically, the candidate will be able to apply data subject rights in relation to:

- 9.1.1 Confirmation of processing
- 9.1.2 The right to be informed (transparency, compatibility of further processing and modalities)
- 9.1.3 Access to personal data including:
  - 9.1.3.1 The process to deal with a request
  - 9.1.3.2 Timescales
- 9.1.4 Protecting the rights of another (third party individual)
- 9.1.5 Rectification
- 9.1.6 Erasure (and the right to be forgotten including the provisions that relate to children)
- 9.1.7 Restriction of processing
- 9.1.8 Obligation to notify the rectification, erasure or restriction to recipients and the data subject
- 9.1.9 Portability
- 9.1.10 Objection and rights in relation to direct marketing
- 9.1.11 Automated individual decision making and profiling
- 9.1.12 Lodging a complaint
- 9.1.13 Effective judicial remedy
- 9.1.14 Compensation

10 Restriction on data subject rights (3 hours, 7.5%, K3)

10.1 The candidate will be able to describe and apply the exemptions from data subject rights, and demonstrate a broad understanding of the exemptions established under Article 23, interpreting how the following can be applied in practice:

- 10.1.1 The importance of the GDPR recitals and how they will be used by the courts
- 10.1.2 Protection of the rights of others
- 10.1.3 Crime and taxation, including:
  - 10.1.3.1 Prevention or detection of crime
  - 10.1.3.2 Apprehension or prosecution of offenders and self-incrimination
  - 10.1.3.3 Disclosures likely to prejudice crime, taxation and the proper discharge of a function designed to protect the public
- 10.1.4 Assessment or collection of a tax, duty or similar imposition
- 10.1.5 Assessment or collection of a tax, duty or similar imposition
- 10.1.6 Border Control
- 10.1.7 Immigration
- 10.1.8 Disclosures prohibited by law:
  - 10.1.8.1 Human fertilisation and embryology
  - 10.1.8.2 Adoption records
- 10.1.9 Processing in connection with legal proceedings, seeking legal advice or exercising or defending legal rights and legal professional privilege
- 10.1.10 Corporate finance
- 10.1.11 Courts and judiciary
- 10.1.12 Management forecasts
- 10.1.13 Negotiations with the data subject
- 10.1.14 Confidential references
- 10.1.15 Health, social work and education (reasonableness test)
  - 10.1.15.1 Child abuse data
  - 10.1.15.2 Education data, examination scripts and marks
- 10.1.16 Scientific or historical research and statistics
- 10.1.17 Freedom of expression
- 10.1.18 Archiving in the public interest

NB: The candidate will not be expected to have a detailed knowledge of all the derogations set out in the GDPR

11 Offences (0.5 hours, 1.25%, K2)

11.1 The candidate will be able to describe the range of offences under UK data protection legislation which are dealt with by the courts, including:

- 11.1.1 How specific offences currently apply in practice
- 11.1.2 The difference between offences and administrative fines
- 11.1.3 The interpretation of 'effective, proportionate and dissuasive' and where the UK intends to legislate for new infringements

11.2 The candidate will be able to demonstrate what constitutes an offence, including:

- 11.2.1 Failure to comply with an information notice
- 11.2.2 Falsely or recklessly responding to an information notice
- 11.2.3 Unlawfully obtaining personal data, knowingly or recklessly to:
  - 11.2.3.1 Obtain or disclose personal data without the consent of the controller(s)
  - 11.2.3.2 Procure the disclosure of personal data to another person without the consent of the controller, or, subsequently retaining or processing the data, without the consent of the person who was the controller when it was obtained
- 11.2.4 Alteration, defacing, blocking, concealing, erasure or destruction of personal data to prevent disclosure under a subject access request
- 11.2.5 Re-identification or use of anonymised/pseudonymised data without the consent of the controller
- 11.2.6 Enforced Subject Access offences (i.e. Prohibition of requirement to produce relevant records in connection with employment and provision of services etc)

12 Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003 (1 hour, 2.50%, K2)

12.1 The candidate will be able to describe the relationship between the current PECR and the broad scope of the GDPR, and interpret the main provisions in relation to unsolicited marketing and consent, including relating to:

- 12.1.1 Unsolicited marketing calls by telephone and role of TPS
- 12.1.2 Marketing calls using pre-recorded message (robotic call consent requirements)
- 12.1.3 Unsolicited marketing emails (including SMS and the soft opt-in)

13 Other associated legislation (1 hour, 2.50%, K2)

13.1 The candidate will be able to identify UK legislation relevant to the implementation of the GDPR.

NB: The candidate will not be expected to have an in-depth knowledge but will be required to explain how UK data protection relates to the following legislation:

- 13.1.1 Computer Misuse Act 1990 (as amended by the Serious Crime Act 2015) Offences:
  - 13.1.1.1 Unauthorised access to computer material
  - 13.1.1.2 Unauthorised access with intent to commit or facilitate commission of further offences (e.g. theft of data)
  - 13.1.1.3 Unauthorised modification to contents of a computer
  - 13.1.1.4 Unauthorised acts with intent to impair operation of a computer
  - 13.1.1.5 Causing or creating risk of serious damage
- 13.1.2 Freedom of Information Act 2000 (FOIA) and Freedom of Information (Scotland) Act 2002 (FOISA)
  - 13.1.2.1 Information exempt from subject access rights and disclosures involving personal data

13.2 The candidate will be able to explain the interaction between UK data protection legislation and the FOIA/FOISA, as well as the Environmental Information Regulations where the fulfilment of a disclosure request may be exempt due to the impact of data protection legislation.

14 Application of data protection legislation (18 hours, 45%, K3)

This topic ensures the candidate is able to recognise the application of compliance in a range of circumstances and apply their knowledge of data protection legislation across a range of detailed scenarios.

14.1 Data controller and data processor obligations: The candidate will be able to apply the requirements relating to Article 5(2) of the GDPR and will be expected to be able to demonstrate practical applications of the following:

- 14.1.1 General obligations of a controller and processor
- 14.1.2 Data controller/data processor and joint controller relationships
- 14.1.3 Accountability and governance
- 14.1.4 Administration and maintaining records of processing activities
- 14.1.5 Notification and consultation with supervisory authorities
- 14.1.6 Published codes of practice (and where applicable codes of conduct) to include:
  - 14.1.6.1 Employment practices code
  - 14.1.6.2 Data sharing code of practice
  - 14.1.6.3 CCTV code of practice
  - 14.1.6.4 Privacy information notices, transparency and control
  - 14.1.6.5 Privacy impact assessment code of practice
  - 14.1.6.6 ICO consent guidelines
  - 14.1.6.7 The role of the WP29/European Data Protection Board in relation to publication of Codes of Conduct

14.2 Security of processing: The candidate will be expected to explain the obligations for securing personal data, including:

- 14.2.1 Organisational and technical security measures
- 14.2.2 Notification of a personal data breach to the supervisory authority
- 14.2.3 Overlap with the NIS Directive in relation to breach reporting
- 14.2.4 Communication of a personal data breach to the data subject
- 14.2.5 Using data protection impact assessments and prior consultation with the supervisory authority
- 14.2.6 Data processor supervision and security in third party contracts
- 14.2.7 Adopting a 'data protection by design/data protection by default' approach when setting security requirements for new processing systems
- 14.2.8 Requirement for education and training

14.3 Data protection officer**:** The candidate will be able to describe the role of the data protection officer as defined in the GDPR and the Data Protection Act 2018, including:

- 14.3.1 Data protection officer designation, position and role/tasks
- 14.3.2 WP29 Guidance on Data Protection Officers (16/EN/WP243:2017e)

14.4 Addressing scenarios in specific sectors: The candidate will be able to interpret how the following sectors may influence the practical implementation of the GDPR:

- 14.4.1 Marketing
- 14.4.2 Financial services
- 14.4.3 Services provided by public bodies (e.g./ Local and Central Government)
- 14.4.4 Human resource management
- 14.4.5 Health sector

14.5 Data processing topics: The candidate will be able to explain how data protection concepts apply to the following business processes:

- 14.5.1 Monitoring and profiling of data subjects – internet, email, telephone calls and CCTV
- 14.5.2 Use of the internet (including electronic commerce)
- 14.5.3 Data matching, data analytics and data warehousing (big data and profiling)
- 14.5.4 Disclosure and data sharing

NB: The focus is on the candidate recognising the practical issues of complying with legislation in the real world. Candidates are encouraged to understand how they would approach different scenarios to become familiar with the practicalities of compliance. Compliance advice on particular topics and for specific sectors is published by the Information Commissioner. It is strongly recommended that human resource management related issues are addressed.

Levels of knowledge / SFIA levels

This course will provide candidates with the levels of difficulty/knowledge skill highlighted within the following table, enabling them to develop the skills to operate at the levels of responsibility indicated.

The levels of knowledge and SFIA levels are explained in on the website www.bcs.org/levels.

The levels of knowledge will also enable candidates to develop the following levels of skill to be able to operate at the following levels of responsibility (as defined within the SFIA framework) within their workplace:

Level	Levels of Knowledge	Levels of Skill and Responsibility (SFIA)
K7		Set strategy, inspire and mobilise
K6	Evaluate	Initiate and influence
K5	Synthesise	Ensure and advise
K4	Analyse	Enable
K3	Apply	Apply
K2	Understand	Assist
K1	Remember	Follow

Format of Examination

Type	20 simple multiple-choice questions (1 mark each) 20 complex multiple-choice questions (2 marks each) and 12 short answer questions (5 marks each)
Duration	2 hours. An additional 30 minutes will be allowed for candidates sitting the examination in a language that is not their native language
Pre-requisites	Accredited training is strongly recommended but is not a prerequisite
Supervised	Yes
Open Book	No
Pass Mark	78/120 (65%)
Distinction Mark	96/120 (80%)
Calculators	Calculators cannot be used during this examination
Learning Hours	40
Delivery	Paper based examination

Trainer Criteria

Criteria	• Hold the BCS Practitioner Certificate in Data Protection • Have 10 days' training experience or hold a train the trainer qualification • Have a minimum of 3 years' experience in the area of data protection • Be familiar with the structure and text of the GDPR and have a comprehensive understanding of its impact upon the practical implementation of data protection compliance.

Classroom size

Trainer to Learner ratio	1:16

Recommended Reading List

IMPORTANT: Legislation, Codes of Practice and Guidance are subject to change. Candidates should ensure they are referring to the most up to date version.

Legislation (can be found at www.legislation.gov.uk)

UK Data Protection Act 2018
(http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf)

The Privacy and Electronic Communications (EC Directive) Regulations 2003
http://www.legislation.gov.uk/uksi/2003/2426/contents/made

Data Protection Directive 95/46/EC
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Information Commissioner's Office Guidance and Codes of Practice
www.ico.org.uk

Information Commissioner's Office Guideline – personal information and the FOIA
https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-9.pdf

The Guide to Data Protection Author: Information Commissioners Office Publisher: Information Commissioners Office
http://ico.org.uk/for_organisations/data_protection/the_guide

EU Regulation 679 General Data Protection Regulations
http://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-679-F1-EN-MAIN.PDF

Information Commissioner's Data Protection Reform Website
www.ico.org.uk/for-organisations/data-protection-reform

Overview of the GDPR
www.ico.org.uk/for-organisations/data-protection-reform

EU Directive EU-2016/680 Law Enforcement
http://eur-lex.europa.eu/homepage.html?locale=en

Codes of Practice

UK ICO Privacy Notices Code of Practice
www.ico.org.uk/for-organisations/data-protection-reform

EU Article- 29 Working Party Guidelines on Data Protection Officers (16-EN-WP243-rev01)
https://ec.europa.eu/commission/index_en

EU Article 29 Working Party Guidelines on Data Processing At Work (employment context
https://ec.europa.eu/commission/index_en

EU Article 29 Working Party Guidelines on the Lead Supervisory Authority (WP-244-rev01)
https://ec.europa.eu/commission/index_en

EU Article 29 Working Party Guidelines on the role of the DPO
https://ec.europa.eu/commission/index_en