BCS Foundation Certificate in Data Protection Syllabus [2017]

Version 2.4
December 2017

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

BCS Foundation Certificate in Data Protection [2017]

Contents

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
Version 2.4 December 2017	Typo, layout and minor amendments. Added version date to title
Version 2.3 December 2017	Added additional reference words in 5.1
Version 2.2 November 2017	Added marking scheme to Format of Examination Table
Version 2.1 November 2017	Amends to article numbers in section 3, 4 and 6
Version 2.0 November 2017	Syllabus amended in line with GDPR and Data Protection Bill
Version 1.2 December 2016	Strapline regarding regulated statement has been added
Version 1.1 March 2015	Updated the extra time requirements – candidates whose first language is not English are entitled to an extra 15 minutes and use of dictionaries
Version 1.0 March 2014	New certification and syllabus created

Introduction

Knowledge of UK data protection law, including the EU General Data Protection Regulation (GDPR) and the UK Data Protection Bill along with an understanding of how they are applied in practice, is important for any organisation processing personal information. The BCS Foundation Certificate in Data Protection is designed for those who wish to acquire a sound grounding in the key elements of the law and its practical application.

Objectives

The Foundation Certificate [2017] is intended to promote an understanding of UK Data Protection law. By obtaining the Foundation Certificate, candidates will:

- Hold a recognised qualification in data protection
- Gain an understanding of the key changes that the GDPR and the Data Protection Bill bring to data protection
- Gain an understanding of individual and organisational responsibilities under the GDPR and the UK Data Protection Bill, particularly the need for effective record keeping
- Gain an understanding of the new rights available to data subjects and the implications of those rights with the GDPR and UK Data Protection Bill
- Gain an understanding of the increased obligations faced by data controllers and data processors as a result of the GDPR coming into force and the Data Protection Bill being enacted
- Be better placed to support their organisation in processing customer data in compliance with the GDPR and the Data Protection Bill.

Target Audience

The qualification is primarily aimed at those who need to have an understanding of data protection, and the GDPR in particular, to do their job, or those whose effectiveness in their role would be enhanced by knowledge of the law in this area.

The Foundation Certificate will also provide a stepping stone for those who have, or who will have, some responsibility for data protection within an organisation and who intend in due course to gain the BCS Practitioner Certificate in Data Protection.

This qualification is likely to be of particular benefit to those working in the following areas:

- Data Protection and Privacy
- Information Governance, risk and compliance
- Data Management
- Project Management
- Legal and procurement
- Marketing

- Information Security
- Human Resources

Course format and duration

Candidates can study for this certificate in two ways: by attending training courses provided by accredited training organisations or by self-study. An accredited training course will require a minimum of 16 hours of study run over a minimum of two 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

This is a foundation level qualification and candidates will not need to have prior knowledge of data protection law (although it would be an advantage). It is strongly recommended that candidates complete an accredited training course but this is not mandatory.

Format the examination

- 60 minutes 'closed-book', i.e. no materials can be taken into the examination room
- 40 multiple choice questions
- Pass mark is 26/40 (65%)

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 training providers

It is required that all courses accredited for the BCS Foundation Certificate in Data Protection will provide a minimum of 16 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(s) 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. Legal background and positioning (1 hour, 6%, K2)

The objective is to ensure the candidate has a basic understanding of 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 UK Data Protection Bill 2017 and will be updated should there be any changes once it is enacted as the new UK Data Protection Act.

1.1 Context of data protection law

The objective is to ensure that the candidate is able to summarise the revised structure, legal context and wider scope of GDPR and its positioning in relation to the current UK Data Protection Act 1998 and the status of the UK Data Protection Bill, including the following:

- **1.1.1** EU Directive 2016/680, the Data Protection Law Enforcement Directive (DPLED)
- **1.1.2** The Privacy and Electronic Communications (EC Directive 2002/58/EC) Regulations 2003
- **1.1.3** UK Human Rights Act 1998
- **1.1.4** EU Charter of fundamental rights and freedoms (Article 8)
- **1.1.5** UK Data Protection Bill, Part 2, Chapters 1 to 3

The candidate is expected to have a basic knowledge of the existence of the above and how UK data protection has evolved. The candidate is not expected to have a detailed knowledge of the provisions.

1.2 The role of the Supervisory Authority (Information Commissioners Office [ICO])

Specifically, the candidate will be expected to be able to identify:

- **1.2.1** Registration (Notification) scheme
- **1.2.2** Information Fee (Section 108, Digital Economy Act 2017)
- **1.2.3** Provision of guidance
- **1.2.4** Codes of practice
- **1.2.5** Enforcement
- **1.2.6** Co-operation between supervisory authorities
- **1.2.7** European Data Protection Board

NB Details of enforcement provisions and specific codes are covered elsewhere in the syllabus.

1.3 Territorial scope and jurisdiction of the GDPR (Articles 2 and 3)

Specifically, the candidate will need to recognise the following:

1.3.1 Main establishment and the one stop shop
1.3.2 When EU representative is needed

1.4 Transfers of personal data outside the EU

Specifically, the candidate will be required to recognise the general principles for transferring personal data to third countries, on the basis of:

1.4.1 An adequacy decision by the EU
1.4.2 Adequate safeguards
- Contractual clauses
- Binding Corporate Rules

1.4.3 Derogations for Special circumstances

2. Identification of processing that must comply with the data protection law (2 hours, 13%, K2)

2.1 Definitions

Specifically, the candidate will be expected to identify the following UK definitions that support the application of the GDPR and the lawfulness of processing:

2.1.1 Personal data
2.1.2 Special category personal data
2.1.3 Processing
2.1.4 Filing system
2.1.5 Data controller
2.1.6 Data processor
2.1.7 Data subject
2.1.8 Public authority, Scottish public authority and public body, (including Crown and Parliament)
2.1.9 Manual unstructured data held by a FOIA/FOISA public authority
2.1.10 Profiling
2.1.11 Pseudonymisation
2.1.12 Consent
2.1.13 Child's consent in relation to information society services
2.1.14 Personal data breach
2.1.15 Processing for purely personal or household purposes exemption

3. Understanding the data protection principles (5 hours, 31%, K2)

The objective is to ensure that the candidate can identify how the six fundamental principles of data protection set out in Article 5(1) of the GDPR regulate the processing of personal data, as well as an understanding of the differences between them. The candidate will also be expected to understand data controller and data processor accountability established in Article 5(2).

3.1 Lawfulness of processing

Specifically, the candidate will need to be able to identify the lawful conditions (grounds) that must be satisfied in order to lawfully process personal data and special categories of personal data described in Article 6 and 9 of the GDPR, including:

- **3.1.1** Conditions for consent (Article 7 and Recitals 32, 42 and 43)
- **3.1.2** Consent of a child in relation to information society services (Article 8)
- **3.1.3** Processing of special category data by a controller bound by legal, professional or other binding obligations of secrecy (common law duty of confidentiality).
  - We are not talking about the Information Commissioner's obligations of secrecy
  - **Note:** refer to Recital 50 "expectations of privacy" by a data subject in relation to further processing and Schedule 1, para 2 (3) and Chapter 2, Part 2 – the GDPR, Section 10, para (1) of the DP Bill
- **3.1.4** Personal data relating to criminal convictions and alleged offences (Article 10)
- **3.1.5** Processing which does not require identification (Article 11)

4. Rights of the Data Subject (2 hours, 13%, K2)

4.1 The objective is to ensure the candidate is able to identify the rights granted to individuals (Articles 12–22). Specifically, the candidate will be required to explain data subject rights in relation to:

- **4.1.1** Confirmation of processing
- **4.1.2** Being informed (transparency), including of further processing compatibility (Article 13 and Article 14)
- **4.1.3** Access to personal data (Article 15)
- **4.1.4** Rectification (Article 16)
- **4.1.5** Erasure (Right to be forgotten) (Article 17)
- **4.1.6** Restriction of processing (Article 18)
- **4.1.7** Obligation to notify the rectification, erasure or restriction to recipients and the data subject (Article 19)
- **4.1.8** Portability (Article 20)
- **4.1.9** Objection and rights in relation to direct marketing (Article 21)
- **4.1.10** Automated individual decision making and profiling (Article 22)

4.1.11 Lodging a complaint (Article 77)
4.1.12 Effective judicial remedy (Article 78 and 79)
4.1.13 Compensation (Article 82)

4.2 Restriction on Data Subject Rights

The candidate is not expected to have a detailed knowledge of restrictions on data subject's rights (Article 23) but will be expected to identify restrictions that may affect data subject rights of access (Article 15), to include:

4.2.1 Protection of the rights of others
4.2.2 Crime and taxation
4.2.3 Prevention or detection of crime
- Apprehension or prosecution of offenders, self-incrimination
- Processing (e.g. disclosures) likely to prejudice crime and taxation
- Assessment or collection of a tax, duty or similar imposition
- Border control
- Immigration
- Disclosures prohibited by law
- National Security

4.2.4 Processing in connection with legal proceedings, seeking legal advice or exercising or defending legal rights and legal professional privilege
4.2.5 Processing likely to prejudice the discharge of statutory functions designed to protect the public (e.g. regulatory functions, ministers of the Crown)
4.2.6 Corporate finance
4.2.7 Courts and judiciary
4.2.8 Management forecasts
4.2.9 Negotiations with the data subject
4.2.10 Confidential references
4.2.11 Health, social work, education
- Child abuse data
- Education data, exam scripts and marks

4.2.12 Research and statistics
4.2.13 Archiving in the public interest

5. Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003 (1 hour, 6%, K2)

The objective is to ensure the candidate can identify the relationship between the PECR and the GDPR, including the PECR's:

5.1 Objective and broad scope (email, phone, SMS, automated calls, robocalls)
5.2 Provisions relating to electronic marketing communications
5.3 ICO Guidance on direct Marketing and Direct Marketing Commission Code
- DMA telephone preference services

5.4 ICO services to the public – Reporting complaints and concerns

6. Data controller and data processor obligations (3 hours, 19%, K2)

The objective is to ensure that the candidate can identify the following controller and processor obligations:

6.1 Accountability and data governance (Article 5 (2))
6.2 Controller obligations (Article 24)
6.3 Data protection by design and by default (Article 25)
6.4 Joint controllers (Article 26)
6.5 Processor obligations (Article 28)
6.6 Processing under the authority of a Controller or Processor (Article 29)
6.7 Records of processing activities (Article 30)
6.8 Co-operation with the ICO (Article 31)
6.9 Information security (Article 32)
6.10 Data breach notification obligations (Articles 33 and 34) to the:
- ICO
- Data subject

6.11 Data protection impact assessment (Article 35)
6.12 Consultation with the ICO on high risk processing (Article 36)
6.13 Data Protection Officer appointment, competency and independence (Article 37 to 39)

7. Enforcement (0.5 hours, 3%, K2)

The objective is to ensure the candidate can indicate how the supervisory authority (ICO) and the courts enforce the provisions of the GDPR and the Data Protection Bill.

Specifically, the candidate will be expected to identify the powers of the ICO (Article 58) in relation to:

7.1 Information notices and assessments
7.2 Undertakings
7.3 Enforcement notices
7.4 Monetary penalty notices (Article 83 and 84)
7.5 Data protection audits by the supervisory authority
7.6 Offences

Candidates will need to understand where enforcement powers apply under the GDPR and be aware of potential changes as the Data Protection Bill is enacted.

8. Codes of Conduct and Best Practice Standards (1.5 hour, 9%, K1)

The candidate will be expected to be aware of the existence of published Codes of Conduct and official guidelines published by the ICO, the importance of using them and the existence of recognised standards that support data protection laws in the UK, including BS10012:2017.

The candidate will be expected to recall what Codes of Conduct are available and the value of using them, but are not expected to know detailed content. Specifically, the candidate will need to be able to identify:

8.1 The status and use of Codes of Conduct

8.2 Published codes in the following key areas:

- Privacy notices
- Subject access
- Employment practices
- CCTV
- Data protection impact assessment
- Business sector codes
- Proposed codes of practice (Data Sharing Code and Direct Marketing Code)
- Useful standards

Levels of knowledge / SFIA levels

This syllabus 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 on the website www.bcs.org/levels.

The levels of knowledge above will 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	Multiple choice, 40 Questions (1 mark each)
Duration	60 minutes. An additional 15 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	26/40 (65%)
Distinction Mark	None
Calculators	Calculators cannot be used during this examination
Learning hours	16 hours
Delivery	Paper based examination

Trainer Criteria

Criteria	▪ Hold the BCS Foundation 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 the Data Protection Bill 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 Conduct 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)

The Data Protection Act 1998
http://www.legislation.gov.uk/ukpga/1998/29/contents

UK Data Protection Bill 2017 https://www.gov.uk/government/collections/data-protection-bill-2017

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

The Guide to Data Protection Author: 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
www.Eur-Lex.europa.eu

Best Practice Standards

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)