BCS Practitioner Certificate in Data Protection

Syllabus v9.3

The Chartered Institute for IT

July 2021

This professional certification is not regulated by the following United Kingdom Regulators – Ofqual, Qualification in Wales CCEA or SQA.

Contents

Copyright © BCS 2021

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
9.3 July 2021	Syllabus amended to reflect Brexit changes enshrined in legislation and current cases.
V9.1 August 2020	Trainer criteria updated
V 9.0 June 2020	Syllabus amended and updated to reflect current status of data protection legislation
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)

Copyright © BCS 2021

Introduction

Knowledge of UK data protection law, incorporating the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018, as well as the EU General Data Protection Regulation (GDPR), along with an understanding of how they are applied in practice, is important for any organisation processing personal information. The BCS Practitioner Certificate in Data Protection 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.

This version of the syllabus has been updated to take into account the UK's withdrawal from the EU, and following the EU-UK Trade and Cooperation Agreement that was signed in December 2020. The UK does not have an adequacy decision in its favour from the EU. Any change to that position will be included in a subsequent update, planned for 30th June 2021.

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 EU GDPR, the UK GDPR and the UK Data Protection Act 2018 have brought to data protection in practice and what needs to be done to steer their organisations towards 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 Certificate 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.

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
- Directors/Senior Managers with Data Protection responsibilities
- Legal and procurement
- Marketing and Sales professionals
- Information Security and IT
- Human Resources

Levels of Knowledge / SFIA Levels

This syllabus will provide candidates with the levels of difficulty / knowledge 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 further explained on the website www.bcs.org/levels.

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

Learning Outcomes

Candidate will be able to demonstrate knowledge and understanding of key provisions of Data Protection legislation in the following areas:

1. Context of data protection legislation.
2. Principles of data protection and applicable terminology
3. Lawful basis for processing of personal data
4. Governance and accountability of data protection within organisations
5. Interaction between Controller and Processor, and role of third parties
6. Transfers of personal data to third countries or international organisations
7. Data Subject Rights
8. The role of the Information Commissioner's Office (ICO) and Independent Supervisory Authorities (ISAs)
9. Breaches, enforcement and liability
10. Processing of personal data in relation to children
11. Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003

Study Format and Duration

Candidates can study for this certificate in two ways:

- Attending an accredited training course. This will require a minimum of 40 hours of study over a minimum of five days.
- Self-study. Self-study resources include online learning and recommended reading (see syllabus Reading List).

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) and candidates will be required to demonstrate the ability to apply the principles and requirements in a work context. Candidates are strongly recommended to have completed an accredited training course. It is also recommended that candidates prepare for the course and examination by committing to personal study before, during and following the course.

Examination Format and Duration

Type	40 Multiple Choice questions
Duration	90 minutes
Supervised	Yes
Open Book	No (no materials can be taken into the examination room)
Passmark	26/40 (65%)
Delivery	Digital or paper based.

Additional Time

For Candidates Requiring Reasonable Adjustments Due to a Disability.

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, then they 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 Organisations

Each major subject heading in this syllabus is assigned a percentage weighting. The purpose of this is:

1) Guidance on the proportion of content allocated to each topic area of an accredited course.
2) Guidance on the proportion of questions in the exam.

Courses do not have to follow the same order as the syllabus and additional exercises may be included, if they add value to the training course.

Question Weighting

Syllabus Area	Syllabus Weighting	Target number of questions per exam
1. Context of data protection legislation.	7.5%	3
2. Principles of data protection and applicable terminology	5%	2
3. Lawful basis for processing of personal data	5%	2
4. Governance and accountability of data protection within organisations	20%	8
5. Interaction between controller and processor, and role of third parties	10%	4
6. Transfers of personal data to third countries or international organisations	2.5%	1
7. Data subject rights	5%	2
8. The role of supervisory authorities (SAs)	7.5%	3
9. Breaches, enforcement and liability	12.5%	5
10. Processing of personal data in relation to children	2.5%	1
11. Specific provisions in data protection legislation of particular relevance to public authorities	7.5%	3
12. Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003	5%	2
13. Application of data protection legislation in key areas of industry	10%	4
Total	**100%**	**40 Questions**

Copyright © BCS 2021

Trainer Criteria

Criteria	• Hold the BCS Practitioner Certificate in Data Protection • Have a minimum of 2 years' training experience or 1 year with a recognised 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 candidate ratio	1:16

Excerpts from BCS Books

Accredited Training Organisations may include excerpts from BCS books in the course materials. If you wish to use excerpts from the books you will need a license from BCS to do this. If you are interested in taking out a licence to use BCS published material, you should contact the Head of Publishing at BCS outlining the material you wish to copy and the use to which it will be put.

Syllabus

Any and all recommended literature and legislation is included to determine the scope of the syllabus and includes any relevant subsections within the Article or Section numbers listed. The Foundation Certificate shall only examine articles and sections listed within the syllabus; however further examples and areas of the legislation may be discussed within the course to provide further context. Please refer to the Recommended Reading List for further guidance on key case law being referenced.

Where terminology is interchangeable within the legislation, candidates will be expected to understand the interchangeable terms for the purpose of their work within industry, however the terminology used within the syllabus will be duplicated within any exam questions produced by BCS.

Learning Objectives

1. Context (7.5%)

Candidates will be able to:

1.1. Explain the concepts of data protection and privacy

1.1.1. Describe an individual's right to private and family life.
1.1.2. Explain the relevance of confidentiality and respect for home and family life and correspondence.

1.2. Describe the history of data protection in the UK, to include:

1.2.1. United Nations Universal Declaration on Human Rights
1.2.2. European Convention on Human Rights and Fundamental Freedoms (ECHR), (Article 8 – Respect for privacy and family life, Article 10 – Freedom of Expression)
1.2.3. Council of Europe Convention 108, 1981, its implementation by the Data Protection Act 1984, and updating of Convention 108
1.2.4. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013
1.2.5. Data Protection Directive 95/46/EC
1.2.6. Human Rights Act 1998
1.2.7. Data Protection Act 1998
1.2.8. Privacy and Electronic Communications Regulation 2002/58/EC (PECR)
1.2.9. General Data Protection Regulation 2016/679
1.2.10. UK Data Protection Act 2018
1.2.11. The purpose of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
1.2.12. UK GDPR

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. Illustrate how the wider territorial scope and jurisdiction of the EU GDPR and UK GDPR impacts on the processing of personal data by global organisations, including those who may not have a business (legal entity) established within the EU or the UK.

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 independent supervisory authorities

1.4. When a representative of the data controller is needed

2. Principles of data protection and applicable terminology (5%)

Candidates will be able to:

2.1. Interpret the major definitions in the GDPR and the Data Protection Act 2018. They should also be 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:

2.1.1. Personal data and Special category personal data
  2.1.1.1. Pseudonymisation
  2.1.1.2. Criminal Offence Data (Article 10 GDPR /Sections 10 & 11 DPA)
  2.1.1.3. Biometric Data
2.1.2. Processing
  2.1.2.1. Profiling
2.1.3. Controller
2.1.4. Processor
2.1.5. Data Subject
2.1.6. Filing system
2.1.7. Recipients and third parties
2.1.8. Purely personal or household purposes
2.1.9. The special purposes

2.2. Demonstrate how the following GDPR principles regulate the processing of Personal Sata and how they are applied:
2.2.1. Lawfulness, Fairness and Transparency - Article 5 (1)(a)
2.2.2. Purpose Limitation - Article 5 (1)(b)
2.2.3. Data minimisation – Article 5(1)(c)
2.2.4. Accuracy – Article 5 (1)(d)
2.2.5. Storage limitation – Article 5 (1)(e)
2.2.6. Integrity and confidentiality – Article 5(1)(f)
2.2.7. Responsibility for accountability with the above principles (referred to as Accountability Principle) - Article 5 (2)

3. **Lawful bases for processing Personal Data (5%)**

Candidates will be able to:

3.1. Illustrate the lawful bases to process personal data listed under (Article 6) of the GDPR and as displayed below:
- 3.1.1. Consent
- 3.1.2. Contract
- 3.1.3. Legal obligation
- 3.1.4. Vital interests
- 3.1.5. Public interest task
- 3.1.6. Legitimate interests

3.2. Describe the conditions for processing special category data and the exemptions (Article 9)

4. **Governance and accountability of data protection within organisations (20%)**

Candidates will be able to:

4.1. Identify the accountability and data governance obligation (Article 5 (2))

4.2. Describe the purpose of a Data Protection Impact Assessment (DPIA)

4.3. Demonstrate the process of conducting a DPIA

4.4. Explain what a record of processing activity (RoPA) is, the information it should contain and why this is important (Article 30)

4.5. Outline the interplay with privacy notices (Article 13 & 14)

4.6. Demonstrate how to adopt a data protection by design and by default approach (Article 25)

4.7. Identify suitable information security measures (Article 32)

4.8. Explain the designation, position and tasks of the Data Protection Officer (DPO) (Article 37 to 39)

5. Interaction between controller and processor, and role of third parties (10%)

Candidates will be able to:

5.1. Explain controller and processor obligations and identify principles (Article 24 & 28)

5.2. Describe the concept of joint controllership (Article 26)

5.3. Describe the act of processing under the authority of a controller or processor (Article 29)

5.4. Explain what a Data Processing Agreement is and when it would be necessary in a controller-processor arrangement

5.5. Identify who would be considered as a recipient or a third party and how this works in practice

6. **Transfers of personal data to third countries or international organisations (2.5%)**

Candidates will be able to:

6.1. Recognise the general principles for transferring personal data to third countries in both the UK and the EU, and illustrate what issues might arise from each of the following mechanisms:

- 6.1.1. An adequacy decision by the EU
  - 6.1.1.1. List of countries deemed adequate by the European Commission
- 6.1.2. An adequacy decision by the UK
- 6.1.3. Appropriate safeguards
  - 6.1.3.1. Standard Contractual Clauses
  - 6.1.3.2. Binding Corporate Rules
  - 6.1.3.3. Derogations (Article 49) and other exemptions (DPA 18 Sections 72-78)

7. Data subject rights (5%)

Candidates will be able to:

7.1. Demonstrate a detailed knowledge of the key rights granted to individuals (Articles 12 to 17 and 21 to 22). Specifically, the candidate will be required to explain data subject rights in relation to:

- 7.1.1. Being informed (transparency), including of further processing compatibility (Article 13 and Article 14)
- 7.1.2. Subject access (Article 15)
  - 7.1.2.1. Prohibition against enforced subject access requests (Section 184 of DPA 18)
  - 7.1.2.2. Void contractual terms relating to health records (Section 185 of DPA 18)
- 7.1.3. Rectification (Article 16)
- 7.1.4. Erasure (Right to be forgotten) (Article 17)
- 7.1.5. Objection (Article 21)
- 7.1.6. Automated individual decision making and profiling (Article 22)

7.2. Express awareness of the following rights in addition to the above. However, these will not be examined in the Practitioner Certificate.

- 7.2.1. Restriction of processing (Article 18)
- 7.2.2. Obligation to notify the rectification, erasure or restriction to recipients and the data subject (Article 19)
- 7.2.3. Portability (Article 20)

7.3. Demonstrate knowledge of the restrictions and exemptions that may affect data subject rights

- 7.3.1. Restrictions (Article 23)
- 7.3.2. Exemptions (Schedule 2 - Parts 1 to 4 of DPA 18)

8. The role of independent supervisory authorities (ISAs) and the ICO (7.5%)

Candidates will be able to:

8.1. Explain the role and importance of supervisory authorities

- 8.1.1. Independence
- 8.1.2. Competence and powers (Article 58 (1) & 58 (2))
- 8.1.3. Co-operation with other supervisory authorities (Articles 60 to 62)
- 8.1.4. Consistency
- 8.1.5. Review of DPIAs in cases of unmitigated high risk (Article 35 & 36)

8.2. Explain the Role of the Information Commissioner's Office (ICO)

- 8.2.1. As a regulator
  - 8.2.1.1. Investigation and correction (Article 58)
  - 8.2.1.2. Enforcement of regulations
  - 8.2.1.3. Data protection audits by the supervisory authority
- 8.2.2. As a body that creates guidance and codes of practice
- 8.2.3. Driving forward good privacy practice in their own jurisdictions and also internationally
- 8.2.4. Promotion of approved privacy seals, certification schemes and availability of commonly used standards
- 8.2.5. Advice and reporting to Parliament, the UK Government and other bodies

8.3. Describe the Role of the European Data Protection Board (EDPB) (Articles 64, 65 & 70)

NB Candidates are expected to have knowledge of the Role of the EDPB however they will not be expected to list the individual tasks in Article 70.

9. Breaches, Enforcement and Liability (12.5%)

Candidates will be able to:

9.1. Explain what constitutes a personal data breach

9.2. Explain when the obligation arises to report breaches of personal data (Articles 33 & 34)

- 9.2.1. To the supervisory authority
- 9.2.2. Data subject

9.3. Explain how a data protection complaint arises (Article 57 (1)(f))

9.4. Describe the sanctions that could be imposed as a result of a personal data breach or data protection complaint:

- 9.4.1. Information notices and assessments
- 9.4.2. Undertakings
- 9.4.3. Enforcement notices (Section 149 DPA 18)
- 9.4.4. Administrative fines and their levels (Article 83 and 84)
  - 9.4.4.1. Tier 1 fines (upto 2% or 10 million euros (or £8.7m under the UK GDPR))

9.4.4.2. Tier 2 fines (up to 4% or 20 million euros (or £17.5m under the UK GDPR)
9.4.4.3. Availability of multiple tiers of fines

9.5. Describe the following liabilities:

9.5.1. Compensation towards the data subject
9.5.2. Liability between controller and processor
9.5.3. Awareness of the existence of criminal liability regarding breaches under the Data Protection Act 2018 (Sections 170 to 173)

9.6. Identify the role of tribunal and judicial courts

9.6.1. Appeals against decisions of the ICO
9.6.2. Adjudication and enforcement of legal claims for data protection breaches

10. **Processing of personal data in relation to children (2.5%)**

Candidates will be able to:

10.1. Explain how data protection legislation applies to children:
10.1.1. Explain the differences between the definitions of "child" within the GDPR (Article 8) and DPA 18 (Section 9)
10.1.2. Explain the concept of erasure (and the right to be forgotten) where it relates to children
10.1.3. Explain what Information Society Services means
10.1.3.1. Age Appropriate Design Code (as published by the ICO under Section 123) (Scope and awareness of principles)

11. Specific provisions in data protection legislation of particular relevance to public authorities (7.5%)

Candidates will be able to:

11.1. Define the meanings of public authority and public body and how it relates to both DPA 18 and the GDPR (Section 7 of DPA 18)

11.1.1. Lawful basis – public interest task (Article 6 (1)(e))
11.1.2. Interplay between availability of legitimate interests (Article 6 (1)(f) and Section 7 (2))

11.2. Explain the provisions relating to Data Protection Officers (DPOs) for public authorities

11.2.1. Mandatory requirement to appoint a DPO (Article 37 (1)(a))

11.3. Explain awareness of the existence of the exemptions for health social work and education (Schedule 3, DPA 18)

11.3.1. Health data
11.3.2. Social work data
11.3.3. Education data, examination scripts and marks
11.3.4. Child abuse data

NB Candidates are expected to have an awareness of the existence of the exemptions but they will not be expected to list or detail the individual exemptions in Schedule 3

12. Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003 (5%)

Candidates will be able to:

12.1. Explain the relationship between PECR and the GDPR, including PECR's:

- 12.1.1. Objective and broad scope (email, phone, SMS, in-app messaging, push notifications)
- 12.1.2. Provisions relating to electronic marketing communications (excluding fax)
- 12.1.3. Role of the ICO in relation to PECR
  - 12.1.3.1. Investigating complaints
  - 12.1.3.2. Issuing codes of practice

12.2. Explain the current status of PECR and the likely future development of this legislation

- 12.2.1. Timeline of draft e-Privacy Regulation
- 12.2.2. Key concepts under draft e-Privacy Regulation
  - 12.2.2.1. Consent
  - 12.2.2.2. Online tracking and digital technologies
- 12.2.3. Application of draft e-Privacy Regulation in the U.K.

13. Application of data protection legislation in key areas of industry (10%)

Candidates will be able to:

13.1. Recognise the data protection implications of the Employment Practices Code

13.2. Describe how the use of CCTV (Data Protection Code of Practice for surveillance cameras and personal information) is governed by data protection law

13.3. Identify how the use of cookies and digital technologies is governed by data protection law

13.4. Explain how data sharing practices are governed by data protection law (ICO Data Sharing Code of Practice)

13.5. Explain the exemptions for journalism and freedom of expression under data protection law

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)

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

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

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

The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
https://www.legislation.gov.uk/uksi/2019/419/contents/made

Other background material

U.K. ICO Guide to Data Protection (GDPR)
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

U.K. ICO Data Sharing Code of Practice
https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/

U.K. ICO Employment Practices Code
https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

U.K. ICO CCTV Code of Practice (Data Protection Code of Practice for surveillance cameras and personal information)
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

U.K. ICO Guide to the Privacy and Electronic Communications (EC Directive) Regulations (PECR)
https://ico.org.uk/for-organisations/guide-to-pecr/

European Data Protection Board (EDPB) (Various guidance notes on GDPR)
https://edpb.europa.eu/edpb_en

U.K. ICO update report on adtech and real time bidding
https://ico.org.uk/about-the-ico/what-we-do/tech-and-innovation/our-work-on-adtech/

Key case law surrounding the concepts of “controller” and “processor” – SWIFT Case

Copyright © BCS 2021

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

Key case law surrounding the controller vs. the data subject and the right to erasure
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

U.K. ICO detailed guidance on subject access requests
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/