BCS Foundation Certificate in Data Protection

Version 3.2

January 2021

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

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 3.2 January 2021	Updated to reflect changes to Privacy Shield in section 6
Version 3.1 August 2020	Corrected trainer requirements
Version 3.0 June 2020	Syllabus amended to reflect current legislation, including Data Protection Act 18 and GDPR in practice.
Version 2.5 April 2019	Renamed Data Protection 2018 for clarity. Amended all refs of DP Bill to Act. Learning objective numbering amended.
Version 2.4 December 2017	Typo, layout and 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 Act 2018, 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 knowledge in the key elements of the law and its practical application.

NB: The syllabus is updated to October 2020, at a time when the UK had left the EU, but an agreement between the UK and EU on its withdrawal has not yet been agreed, and the implementation of the UK GDPR legislation has not yet come into effect. This version of the syllabus reflects the law as at October 2020. Updates made to legislation between October 2020 and May 2021 will be reflected in an update made in July 2021. 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.

Target Audience

This 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
- 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

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

1. An Introduction to the History of Data Protection in the U.K.
2. Principles of Data Protection and Applicable Terminology
3. Lawful bases for processing of Personal Data
4. Governance and Accountability of Data Protection within organisations
5. Controller and Processor obligations
6. Transfers of personal data to third countries or international organisations
7. Data Subject Rights
8. Independent Supervisory Authority (ICO)
9. Breaches, Enforcement and Liability
10. 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 18 hours of study over a minimum of three days.
- Self-study. Self-study resources include online learning and recommended reading (see syllabus Reading List).

Eligibility for the Examination

There are no specific pre-requisites for entry to the examination although accredited training is strongly recommended.

Examination Format and Duration

Type	40 Multiple Choice questions
Duration	60 minutes
Supervised	Yes
Open Book	No (no materials can be taken into the examination room)
Pass mark	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. An Introduction to the History of Data Protection in the U.K.	5%	2
2. Principles of Data Protection and Applicable Terminology	15%	6
3. Lawful bases for processing Personal Data	12.5%	5
4. Governance and Accountability of Data Protection within organisations	20%	8
5. Interaction between Controller and Processor	7.5%	3
6. Transfers of personal data to third countries or international organisations	5%	2
7. Data Subject Rights	12.5%	5
8. Independent Supervisory Authority (ICO)	10%	4
9. Breaches, Enforcement and Liability	10%	4
10. Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003	2.5%	1
Total	**100%**	**40 Questions**

Trainer Criteria

Criteria	• Hold the BCS Foundation 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' practical experience in the relevant subject area

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

The syllabus is updated to October 2020, at a time when the UK had left the EU, but an agreement between the UK and EU on its withdrawal has not yet been agreed, and the implementation of the UK GDPR legislation has not yet come into effect. This version of the syllabus reflects the law as at October 2020. Updates made to legislation between October 2020 and May 2021 will be reflected in an update made in July 2021. 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.

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 areas of the legislation may be discussed within the course to provide further context.

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. An Introduction to the History of Data Protection in the U.K. (5%)

Candidates will be able to:

1.1. Demonstrate an awareness around personal data rights in the EU and the UK:
- 1.1.1. Background to the Rights to Protect Personal Data in the EU and the U.K.
- 1.1.2. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (Sections 5-26)
- 1.1.3. UK Data Protection Act 2018, Part 2, Chapters 1 to 3, Part 5 & 6

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

1.2. Recognise the territorial scope and jurisdiction of the GDPR (Articles 2 and 3): specifically, the following:
- 1.2.1. Main establishment and the one stop shop
- 1.2.2. When an EU representative is needed

2. Principles of Data Protection and Applicable Terminology (15%)

Candidates will be able to:

2.1. Define the following key items of terminology:
- 2.1.1. Personal data and Special category personal data
  - 2.1.1.1. Pseudonymisation
  - 2.1.1.2. Criminal Offence Data (Article 10/Section 10 & 11 – recitals in relation to)
  - 2.1.1.3. Biometric Data
- 2.1.2. Processing
- 2.1.3. Controller
- 2.1.4. Processor
- 2.1.5. Data Subject
- 2.1.6. Profiling

2.2. Describe the following Data Protection Principles:
- 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 of Personal Data (12.5%)

Candidates will be able to:

3.1. Explain the lawful basis 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)

Governance and Accountability of Data Protection within organisations (20%)

Candidates will be able to:

4.1. Identify the accountability obligations (Article 5 (2) and Article 24)
4.2. Describe the purpose of a Data Protection Impact Assessment (DPIA)
4.3. Explain the process of conducting a DPIA
4.4. Identify the importance of keeping a record of processing activity (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)

Interaction between Controller and Processor (7.5%)

Candidates will be able to:

5.1. Identify the following controller and processor obligations
- 5.1.1. Controller obligations (Article 24)
- 5.1.2. Joint controllers (Article 26)
- 5.1.3. Processor obligations (Article 28)
- 5.1.4. Processing under the authority of a Controller or Processor (Article 29)

Transfers of personal data to third countries or international organisations (5%)

Candidates will be able to:

6.1. Recognise the general principles for transferring personal data to third countries, based on the most common forms:
- 6.1.1. An adequacy decision by the EU
- 6.1.2. Appropriate safeguards
  - 6.1.2.1. Standard Contractual Clauses
    - 6.1.2.1.1. Schrems II
  - 6.1.2.2. Binding Corporate Rules

N.B. The Privacy Shield is no longer a valid legal mechanism for the transfer of personal data from the EU to the US. However, many organisations are still using this mechanism until the EU updates its Standard Contractual Clauses. The *Schrems II* decision adds in an obligation for those using SCCs to assess the level of protection offered by the data protection laws of the receiving party.

Data Subject Rights (12.5%)

Candidates will be able to:

7.1. Explain 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)
7.1.3. 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 Foundation 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. Define restrictions that may affect data subject rights however they are not expected to have a detailed knowledge of these restrictions (Article 23).

Independent Supervisory Authority (ICO) (10%)

Candidates will be able to:

8.1. Explain the Role of the ICO

8.1.1. As a regulator
8.1.1.1. Investigation and correction (Article 58)
8.1.1.2. Enforcement of regulations
8.1.2. As a body that creates guidance and codes of practice
8.1.3. In co-operation with other supervisory authorities
8.1.4. Driving forward good privacy practice in their own jurisdictions and also internationally

Breaches, Enforcement and Liability (10%)

Candidates will be able to:

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

9.1.1. To the Supervisory Authority
9.1.2. Data subject

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

9.2.1. Information notices (Section 142 DPA18) and assessment notices (Section 146 DPA18)
9.2.2. Undertakings
9.2.3. Enforcement notices
9.2.4. Administrative fines and their levels (Article 83 and 84)
9.2.5. Data protection audits by the supervisory authority (Article 58)

9.3. Describe the following liabilities:
9.3.1. Compensation towards the data subject
9.3.2. Liability between controller and processor
9.3.3. Awareness of the existence of criminal liability regarding breaches under:
9.3.3.1. Data Protection Act 2018
9.3.3.2. Computer Misuse Act (Section 3ZA)

Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003 (2.5%)

Candidates will be able to:

10.1. Identify the relationship between the PECR and the GDPR, including the PECR's:
10.1.1. Objective and broad scope (email, phone, SMS, in-app messaging, push notifications)
10.1.2. Provisions relating to electronic marketing communications
10.1.3. Role of the ICO in relation to PECR
10.1.3.1. Investigating complaints

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

The 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 Guide to Data Sharing (Draft) (Pages 16 to 30, 51)
https://ico.org.uk/media/about-the-ico/consultations/2615361/data-sharing-code-for-public-consultation.pdf

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

U.K. ICO Code of Practice on Direct Marketing (Draft code for consultation) (Pages 1 to 40)
https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf

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

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/