BCS GDPR Update: Practitioner Certificate in Data Protection

Version 1.3
November 2017

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

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
V1.3 November 2017	Added marking scheme to Format of Examination table
V 1.2 November 2017	Amends to article numbers in section 3, 5, 6 and 7
V 1.1 November 2017	Timings and weighting changed for Data subject rights to match foundation and weighting amended for practical workshop
V 1.0 November 2017	Certificate and syllabus created

Introduction

Knowledge of UK data protection law, and an understanding of how it is applied in practice, is important for any organisation processing personal data. In May 2018, the EU General Data Protection Regulation (GDPR) becomes fully enforceable across all 28 member states in the European Union. Within the UK, the Government published in September 2017 a Data Protection Bill which once enacted in 2018, will fully incorporate the requirements of the GDPR. This GDPR Update is designed for holders of the BCS Practitioner Certificate in Data Protection who wish to gain a solid understanding of the requirements of the BCS GDPR and the UK Data Protection Bill.

Objectives

The BCS GDPR Update: Practitioner Certificate in Data Protection is intended to provide a comprehensive update for BCS Practitioner Certificate holders. By obtaining the GDPR Update qualification, candidates will:

- Hold an up to date recognised qualification in data protection
- Gain an understanding of the key changes and associated implications that the GDPR introduces for their organisations
- Be prepared for the UK adoption of the GDPR with the enactment of the Data Protection Bill
- Gain an understanding of the practical application of the new requirements of the GDPR and Data Protection Bill associated with the role of the data protection officer (DPO), restrictions of data subject rights, data protection by design and by default and data breach notifications.

Target Audience

The qualification is aimed at holders of the BCS Practitioner Certificate in Data Protection who need to understand the GDPR and the UK Data Protection Bill and the changes that they will bring in the processing of personal data. It is important to those who need to possess an understanding of the GDPR to do their job, or those whose effectiveness in their role would be enhanced by being able to practically apply certain new requirements.

Course Format and Duration

Candidates can study for this certificate in two ways: by attending accredited training courses or by self-study. An accredited training course will require a minimum of 8 hours of classroom tuition followed by four hours of practical exercises and classroom discussion. It is estimated that 20 hours of self-study will be required to attain this certificate. The course can be delivered through traditional classroom-based training or through online e-learning.

Eligibility for the Examination

This is a practitioner level qualification and candidates will need to hold the BCS Practitioner Certificate in Data Protection. It is strongly recommended that candidates complete an accredited training course and exercise workshop although this is not a mandatory requirement for enrolling on the GDPR Update: Practitioner Certificate in Data Protection.

Format and Duration of the Examination

- 1 hour 'closed-book', i.e. no materials can be taken into the examination room
- 15 multiple choice questions
- 6 short answer questions
- Pass mark is 39/60 (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 Accredited Training Providers

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. General Data Protection Regulation (GDPR) background (0.5 hours, 5%, K2)

The candidate will be expected to define the wider scope and jurisdiction of the GDPR, its relationship to the UK Data Protection Bill 2017 (DPB) and other overlapping new or emerging legislation including the following:

- **1.1** Wider scope of the GDPR – EU Directive 2016/679
- **1.2** Main establishment and when EU representation is needed
- **1.3** Cooperation between supervisory authorities (concept of the one stop shop)
- **1.4** UK Data Protection Bill 2017 (implementing the GDPR in the UK) structure and status
- **1.5** EU Directive 2016/680 The Law Enforcement Directive (LED)
- **1.6** The Digital Economy Act 2017
- **1.7** The Directive on Security of Network and Information Systems (NIS Directive) ((EU) 2016/1148)
- **1.8** Telecommunications Directive 97/66/EC, Privacy and Electronic Communications Directive 20002/58/EC, and anticipated revisions (ePrivacy Regulation 2017/0003 (COD)

The candidate will be expected to summarise the above legal instruments and how they relate to or influence the requirements of the GDPR. Candidates are not expected to have a detailed knowledge of their provisions.

2. GDPR definitions and terminology (0.5 hours, 5%)

The objective is to ensure that the candidate is able to distinguish the important definitions in the GDPR where the terminology is new, or differs from previous data protection legislation, including:

- **2.1** Special category personal data
- **2.2** Main establishment
- **2.3** Data minimisation
- **2.4** Data Protection Officer
- **2.5** Data Protection Impact Assessment
- **2.6** Codes of Conduct (Codes of Practice in DPB)
- **2.7** Transparency
- **2.8** Profiling
- **2.9** Consent
- **2.10** Child's consent in relation to information society services
- **2.11** Competent authority in relation to the LED

3. The data protection principles (0.5 hours, 5%, K2)

The objective is to ensure that the candidate can identify how the enhancements to the data protection principles established in the GDPR (Article 5) differ from the UK Data Protection Act 1998 principles, i.e. the 6 principles detailed within Article 5(1) and the accountability requirement from Article 5(2). The candidate will be expected to explain the importance of data processing, specifically:

- **3.1** Transparency requirements in relation to being 'fair and lawful'
- **3.2** Explicit and compatible in relation to 'specified purposes'
- **3.3** Limited to what is 'accurate and relevant'
- **3.4** Pseudonymisation in relation to 'retention'

The candidate will also be expected to also explain the importance of data controllers and processors being accountable for compliance with data processing principles.

4. Special categories of personal data (0.5 hours, 5%, K1)

The objective is to ensure that the candidate recognises that the GDPR introduces new special categories of personal data and separates the processing of personal data relating to criminal convictions and alleged criminal offences, specifically:

- **4.1** Genetic and biometric data
- **4.2** Processing personal information relating to crime as a 'competent authority'
- **4.3** Processing criminal records and alleged offences information in the employment context

5. Lawfulness of processing (1.5 hours, 14%, K2)

The objective is to ensure that the candidate can identify the lawful conditions (grounds) that must be satisfied in order to legitimise the processing of personal data including**:**

- **5.1** Conditions for consent (Article 7, Recitals 32, 42, 43)
- **5.2** Consent of a child in relation to information society services (Article 8)
- **5.3** Special categories of personal data (Article 9 and 10)
- **5.4** Obligations of professional secrecy
- **5.5** Processing that does not require identification (Article 11)

6. Data Subject Rights (1.5 hours, 14%, K2)

The objective is to ensure the candidate is able to identify data subject rights granted under the GDPR, how they relate to the fundamental data processing principles and how they are applied in practice:

- **6.1** Confirmation of processing (Article 12)
- **6.2** Right to be informed (transparency), including of further processing (Article 12, 13 and 14)
- **6.3** Right of access to personal data (Article 15), including timescales
- **6.4** Right to rectification (Article 16)
- **6.5** Right to erasure (to be forgotten) (Article 17)
- **6.6** Right to restriction of processing (Article 18)
- **6.7** Obligation to notify the rectification, erasure or restriction to recipients and the data subject (Article 19)
- **6.8** Right to portability (Article 20)
- **6.9** Right to object and rights in relation to direct marketing (Article 21)
  - Consent rules and the proposed alignment of Privacy In Electronic Communications Regulations (PECR)
- **6.10** Rights in relation to automated decision making and profiling (Article 22)
- **6.11** Right to lodge a complaint (Article 77)
- **6.12** Right to effective judicial remedy (Article 78 and 79)
- **6.13** Right to compensation including non-material damage (Article 82)

7. Data controller and data processor obligations (1 hour, 9%, K2)

The candidate will be required to identify the obligations that are placed upon data controllers and processors under the GDPR, including:

- **7.1** General obligations of a controller and processor (Article 5(2))
- **7.2** Data controller/data processor and joint controller relationships (Article 5(2))
- **7.3** Accountability and governance (Article 5(2))
- **7.4** Controller specific obligations (Article 24)
  - Joint controller obligations (Article 26)
  - Data protection by design and by default (Article 25)
- **7.5** Processor specific obligations (Article 28)
  - Records of processing activities (Article 30)
- **7.6** Information security (Article 32)
- **7.7** Data breach notification (Articles 33 and 34)
  - To the Supervisory Authority including when to notify to the data subject
  - Overlap with the NIS Directive in relation to breach reporting
- **7.8** Data protection impact assessment (Article 35)
- **7.9** Co-operation with the Supervisory Authority (Article 31) and consultation on high risk processing (Article 36)
- **7.10** Data Protection Officer appointment (Article 37 to 39)
- **7.11** Status and use of Codes of Conduct (Article 40)

8. Transfers of personal data (0.5 hours, 5%, K2)

The candidate will be required to identify the:

8.1 General principles for transfers
8.2 Transfers on the basis of an adequacy decision by the EU, including Privacy Shield
8.3 Transfers subject to appropriate safeguards
- Contract clauses
- Binding Corporate Rules

8.4 Exemptions for specific situations

9. Powers of the Supervisory Authority (ICO) (0.5 hours, 5%, K1)

The objective is to ensure the candidate can define the Supervisory Authority's powers to**:**

9.1 Impose monetary penalties
9.2 Issue enforcement notices
9.3 Require controllers or processors to provide information

10. Practitioner level practical workshop (4 hours, 33%, K3)

The objective is to ensure that the Practitioner level candidates understand the practical application of the new requirements of the GDPR and the Data Protection Bill where it varies from the GDPR. Specifically, the candidate will be expected to be able to apply the following requirements to a range of scenarios.

10.1 The role of the Data Protection Officer (DPO)
10.2 Restrictions of data subject rights
10.3 Data protection by design and by default
- How to perform a data protection impact assessment (DPIA)
- Implications for information technology teams
- Evaluation and management of third party contracts (Article 29)

10.4 Personal data breach notifications

To assist the candidate, the workshop will include a range of practical exercises with classroom feedback.

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	Section A: 15 Multiple Choice Questions (2 marks each) Section B: 6 Short Answer Questions (5 marks each)
Duration	1 hour. Candidates will be entitled to an additional 15 minutes if they are sitting the examination in a language that is not their native language.
Pre-requisites	Candidates must hold the BCS Practitioner Certificate in Data Protection Accredited training is strongly recommended but is not a prerequisite
Supervised	Yes
Open Book	No
Pass Mark	39/60 (65 %)
Distinction Mark	None
Calculators	Calculators cannot be used during this examination
Learning Hours	8 hours of classroom tuition and 4 hours of practical exercises and classroom discussion
Delivery	Paper based examination only

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 the Data Protection Bill and have a comprehensive understanding of its impact on organisational and technical measures required in order to comply with the GDPR.

Classroom size

Trainer to candidate ratio	1:16

Recommended Reading and Resource List

This section lists some of the published material available on the GDPR. Candidates are not expected to study all of this material, but should use selected publications to enhance their knowledge. Accredited training providers should recommend appropriate material and resources to supplement their course material to meet syllabus requirements where necessary.

IMPORTANT: Legislation, Codes of Practice and publications are subject to change. There is no guarantee that the information included here is the latest version and candidates are advised to check to ensure that they are referring to the current version.

EU Regulation 2016/679 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)

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

Codes of Conduct

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)