The Chartered Institute for IT

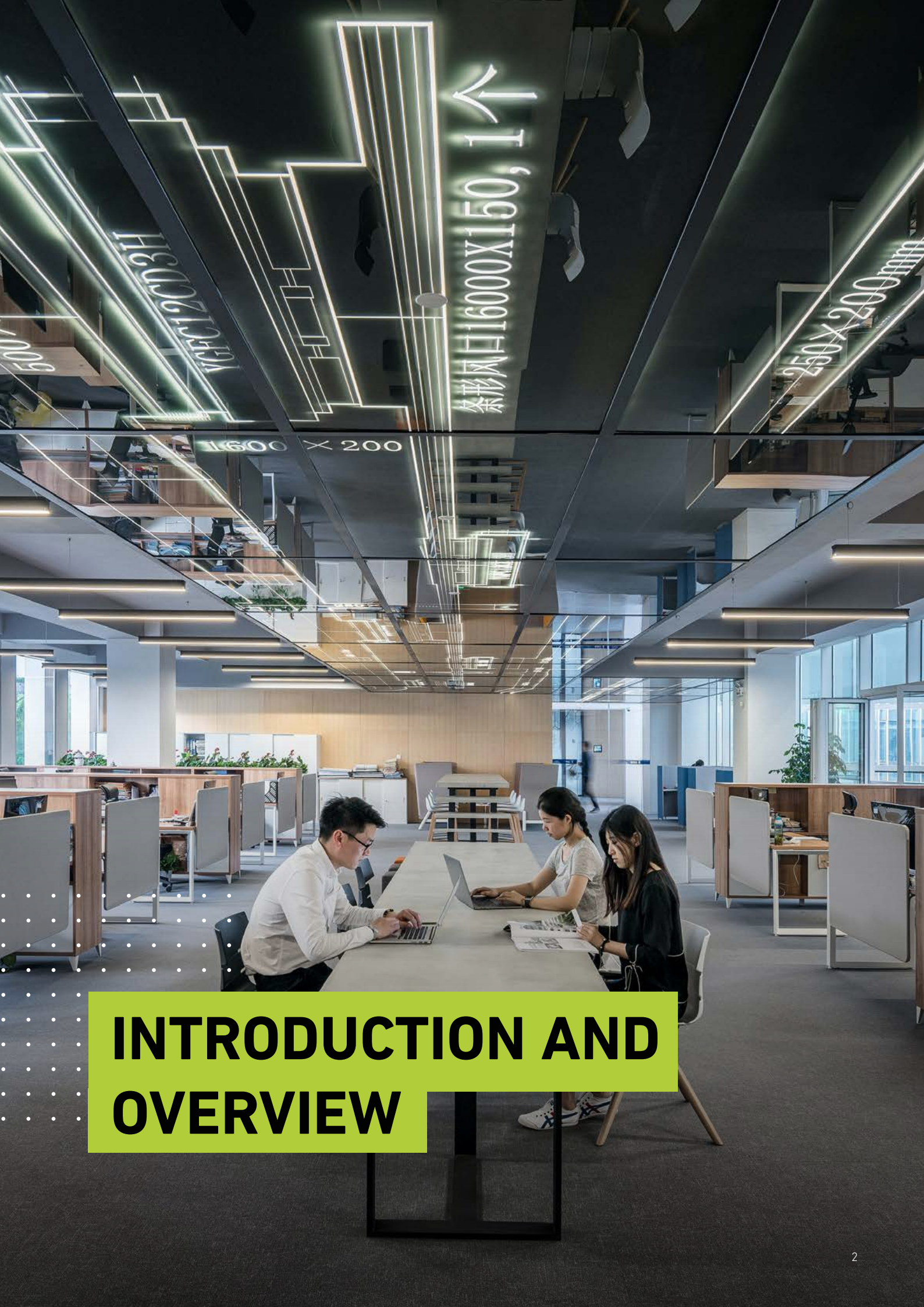
2023 | JAN V3.6

BCS FOUNDATION CERTIFICATE
IN DATA PROTECTION V3.6

SYLLABUS

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

CONTENTS



INTRODUCTION AND OVERVIEW

INTRODUCTION

Knowledge of UK data protection law, incorporating the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, as well as the EU General Data Protection Regulation (EU GDPR), 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 an in depth grounding in the key elements of the UK law and its practical application.

This version of the syllabus has been mapped to the Knowledge, Skills and Behaviours (KSBs) in the Level 4 Data Protection and Information Governance Practitioner apprenticeship standard in tandem with a Subject Matter Expert who is part of the trailblazer group for this standard.

LEARNING OUTCOMES

The candidate should be able to demonstrate knowledge and understanding of key provisions of Data Protection legislation in the following areas:

- An Introduction to the History of Data Protection in the U.K.
- Principles of data protection and applicable terminology.
- Lawful bases for processing of Personal Data.
- Accountability Principle.
- Obligations of Controllers, Joint Controllers and Data Processors.
- International Data Transfers under UK GDPR.
- Data Subject Rights.
- Independent Supervisory Authorities (ISAs) and the Information Commissioner's Office (ICO).
- Breaches, Enforcement and Liability.
- Privacy and Electronic Communications (EC Directive). Regulations (PECR) 2003 and subsequent amendments.

CERTIFICATION SUITABILITY AND OVERVIEW

There are no mandatory requirements for candidates to be able to undertake this certificate, although candidates will need a good standard of written English and Maths. Centres must ensure that learners have the potential and opportunity to gain the certification successfully.

This certificate 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 certification can also support learners taking the L4 Data Protection and Information Governance Practitioner apprenticeship standard by supporting their studies and providing a professional development route (through practitioner and beyond).

This certification 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

Candidates can study for this award by attending a training course provided by a BCS accredited Training Provider or through self-study.

TOTAL QUALIFICATION TIME	ASSESSMENT TIME
23.5 hours	60 minutes

TRAINER CRITERIA

It is recommended that to deliver this award effectively, trainers should possess:

- Hold the BCS Foundation Certificate in Data Protection.
- Have a minimum of 2 years' training experience or 1 year with a recognised qualification.
- A minimum of 3 years of practical experience in the subject area.

SYLLABUS

SYLLABUS

1. AN INTRODUCTION TO THE HISTORY OF DATA PROTECTION IN THE U.K. (6%) (K1, K16, S7, S9)

1.1 Demonstrate an awareness around personal data rights in the EU and the UK.

Indicative content

a. Background to the rights to protect Personal Data in the EU and the UK.
b. General Data Protection Regulation 2016/679.
c. UK GDPR.
d. UK Data Protection Act 2018, Part 2, Chapters 1 to 3, Parts 5 & 6.

Guidance

What do data protection and privacy mean? Why is data protection important? The candidate is expected to be able to identify and explain the indicative content and how UK data protection has evolved, but the candidate is not expected to have a detailed knowledge of the provisions.

1.2 Describe the territorial scope and jurisdiction of the UK GDPR (Article 3).

Indicative content

a. Understand the extent of the territorial scope and the jurisdiction of UK GDPR.
b. How this aligns with the EU GDPR.

Guidance

The candidate should be able to explain that UK GDPR mirrors EU GDPR, and this means that where provisions that apply to the EU, now apply to the UK. Article 3 UK GDPR: The Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the United Kingdom regardless of whether the processing takes place in the United Kingdom or not.

SYLLABUS

2 PRINCIPLES OF DATA PROTECTION AND APPLICABLE TERMINOLOGY. (15%) (K1, K3, S2, S8, S9)

2.1 Define the following key items of terminology:

Indicative content

a. Personal data.
b. Special Category data.
c. Biometric and Genetic data.
d. Criminal Offence data (Article 10 UK GDPR/ Section 10& 11 DPA 2018).
e. Processing of personal data – including scope of processing (Article 2 UK GDPR).
f. Pseudonymisation and anonymisation.
g. Profiling.
h. Data subject.
i. Controller.
j. Data Processor.
k. Recipients and third parties.
l. Filing system.
m. Cross border processing.

Guidance

The candidate must be able to explain the meaning of all the terminology and definitions (Article 4). They should also be able to explain pseudonymisation and anonymisation in terms of whether it is personal data under UK GDPR Article 2.1.2.2.

2.2 Describe the following data protection principles.

Indicative content

a. Lawfulness, fairness and transparency - Article 5 (1)(a).
b. Purpose limitation - Article 5 (1)(b).
c. Data minimisation – Article 5(1)(c).
d. Accuracy – Article 5(1)(d).
e. Storage limitation – Article 5 (1)(e).
f. Integrity and confidentiality – Article 5 (1)(f).

Guidance

Candidates should be able to describe the data protection principles below:

1. Fair, lawful, and transparent: do you have a lawful reason in the first place? Have you communicated with and consulted data subjects (transparency)?

2. Purpose limitation: is your purpose for processing the data clear? Have you documented this?

3. Data minimisation: are you collecting only what you need for your purpose?

4. Accuracy: is the data accurate? Do you have ways of checking and correcting accuracy?

5. Storage limitation: are you storing data only for as long as you need to in line with your purpose? Have you defined a retention period? Do you have methods for securely deleting the data at the end of your retention period?

6. Integrity & confidentiality: Do you have appropriate security measures, policies, and practices?

SYLLABUS

3. LAWFUL BASES FOR PROCESSING OF PERSONAL DATA. (10%) (K1, K14, S2, S7, S13)

3.1 Explain the lawful basis to process Personal Data listed under (Article 6) of the UK GDPR and as displayed below:

Indicative content

a. Consent.
b. Contract.
c. Legal obligation.
d. Vital interests.
e. Public interest task.
f. Legitimate interests.

Guidance

The candidate should be able to explain that consent has to be freely given, specific, informed, and unambiguous and can be withdrawn. Contractual obligation will apply for all types of contract but only where the processing is part of the contract e.g. retail transactions, but not marketing emails. Legal obligation relates to any requirement by law. Vital interests usually means where other lawful basis are unable to be gained e.g. life or death scenarios. Public interest task does not mean everything that a public authority does. Legitimate Interests is often a "catch-all" but if it is the chosen lawful basis, a further type of risk assessment, known as a "Legitimate Interests Assessment" (LIA) must be undertaken.

3.2 Describe the conditions permitted for processing special category data listed under Article 9 of UK GDPR.

Indicative content

a. Identify which of the above also require additional conditions and safeguards as part of Schedule 1 of the DPA 2018.
b. Schedule 2 Public Interest.

Guidance

The candidate should be able to identify where there is the need to meet additional conditions and safeguards from DPA 2018. Criminal Offence Data processing will not be covered in Foundation.

SYLLABUS

4. ACCOUNTABILITY PRINCIPLE. (21.5%) (K1, K2, K3, K4, K6, K8, K14, K15, K16, S1, S2, S9, S10, S11, S12, S13, B3, B4)

4.1 Identify the accountability obligations (Article 5 (2) and Article 24) UK GDPR.

Indicative content

a. Article 5(2): a controller must demonstrate compliance with the data protection principles = accountability.
b. Article 24: Responsibility of the controller.

Guidance

Accountability is an essential part of GDPR compliance; organisations must not only ensure data is safe and secure, but they must also be able to demonstrate this. The candidate should be able to explain the responsibility of the controller including technical measures e.g. encryption and organisational measures (staff policies and procedures, role-based responsibilities and access to data, governance and decision-making provisions.) Please see the UK GDPR text for further details on Articles 24 -39.

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

Indicative content

a. The legal requirement of when to conduct a DPIA.
b. Assessing levels of risk.

Guidance

The candidate should be able to understand the legal; requirements of when to conduct a DPIA of certain types of high-risk data. They should also be able to demonstrate how high-risk data is assessed.

4.3 Explain the process of conducting a DPIA (Article 35) UK GDPR and identify when risks arising from a DPIA may need prior consultation with the ICO (Article 36) UK GDPR.

Indicative content

a. What is included in a DPIA.
b. What needs to be recorded for a DPIA.
c. Consultation with the ICO.

Guidance

The candidate should be able to explain the process of a DPIA and what needs to be documented. They should also identify when there is a legal requirement to consult the ICO prior to the data processing in the DPIA.

4.4 Identify the importance of keeping a record of processing activity (RoPA) (Article 30) UK GDPR.

Indicative content

a. Article 30(1) controller obligations.
b. Article 30(2) processors.
c. RoPA.

Guidance

The candidate should be able to identify and explain controller and processor obligations according to Article 30. They should understand that RoPA is a record of processing activities and that every processing activity requires an entry on RoPA. The RoPA is an important dynamic document (usually an Excel spreadsheet or an online dedicated tool) that the ICO will ask for in the event of an investigation or an audit.

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

Indicative content

a. The individual's right to be informed and the privacy notice.
b. Collecting personal data from individuals both directly and from a 3rd party.

Guidance

The individual's right to be informed about the collection of their personal data. The candidate should be able to outline when to show a privacy notice, the data it should contain, and how it should be structured.

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

Indicative content

a. Identify that these steps must be taken at the time of determining the means for processing.
b. Risk-based approach.

Guidance

The candidate should be able to demonstrate that Article 25 takes Article 24 further, but crucially states that these steps must be taken at the time of determining the means for processing. This is right at the outset of the processing activity, not as an after-thought when the processing has already commenced. Article 25 also introduces the idea that this is a risk-based approach: taking into consideration the nature and scope of the processing and weighing this up against the available technology and cost of implementation.

4.7 Identify suitable information security measures (Article 32) UK GDPR.

Indicative content	Guidance
a. Technical measures. b. Organisational measures.	The candidate should be able to explain what security measures (technical and organisational) controllers and processors must take to secure data.

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

Indicative content	Guidance
a. The role of the DPO. b. Tasks of the DPO.	The candidate should be able to explain the designation, position and tasks of the DPO under UK GDPR.

4.9 Explain the role of the DPO and compliance monitoring.

Indicative content	Guidance
a. DPO's responsibility to monitor data protection compliance. b. Requirements for data protection accountability framework.	Candidates should understand the importance of the DPO role in monitoring compliance, managing risks, and recording and reporting improvements in practices associated with data processing (Article 39 1.b and 2) UK GDP.

SYLLABUS

5. OBLIGATIONS OF CONTROLLERS, JOINT CONTROLLERS AND DATA PROCESSORS. (7.5%) (K1)

5.1 Identify the controller and processor obligations.

Indicative content

a. Controller obligations (Article 24) UK GDPR.
b. Joint controllers (Article 26) UK GDPR.
c. Processor obligations (Article 28) UK GDPR.
d. Processing under the authority of a Controller or Processor (Article 29) UK GDPR.

Guidance

The candidate should be able to explain the differences between controllers, joint controllers and processors, and their respective obligations.

SYLLABUS

6. INTERNATIONAL DATA TRANSFERS UNDER UK GDPR. (7.5%) (K1)

6.1 Explain the principles of data transfers under UK GDPR and the impact of data transfers to and from the European Economic Area (EEA).

Indicative content

a. Identify the principles of what amounts to a data transfer under UK GDPR.
b. Explain the impact of data transfers to and from the EEA as a result of Brexit.
c. Demonstrate a knowledge of the concept of "restricted transfers" and the mechanisms for ensuring these are undertaken lawfully.

Guidance

The candidate should be aware of the current data transfer regime, changes since Brexit and ongoing change.

SYLLABUS

7. DATA SUBJECT RIGHTS. (12.5%) (K7, S4)

7.1 Explain the key rights granted to individuals (Articles 12 to 17 and 21 to 22) UK GDPR. Specifically, the candidate will be required to explain data subject rights in relation to:

Indicative content

a. Being informed (transparency), including of further processing compatibility (Article 13 and Article 14) UK GDPR.
b. Subject access (Article 15) UK GDPR.
c. Rectification (Article 16) UK GDPR.
d. Erasure (Right to be forgotten) (Article 17) UK GDPR.
e. Objection (Article 21) UK GDPR.
f. Automated individual decision making and profiling (Article 22) UK GDPR.

Guidance

Candidate should be able to identify the different rights for individuals regarding their personal data under UK GDPR.

SYLLABUS

8. INDEPENDENT SUPERVISORY AUTHORITIES (ISAS) AND THE INFORMATION COMMISSIONER'S OFFICE (ICO). (7.5%) (K12, K14)

8.1 Express awareness of the role of ISAs under EU GDPR. (Article 57 & 58 EU GDPR).

Indicative content

a. The role of ISAs under EU GDPR.
b. Tasks (Article 57) EU GDPR.
c. Powers (Article 58) EU GDPR.
d. Co-operation between ISAs (Article 60) EU GDPR.

Guidance

Explain the role of the ISA under EU GDPR.

8.2 Explain the role of the ICO.

Indicative content

a. Explain the tasks of the ICO (Article 57 UK GDPR).
b. Explain the powers of the ICO (Article 58 UK GDPR).

Guidance

Candidate should understand the role of the ICO as the data protection regulator and the impact of their tasks and powers.

SYLLABUS

9. BREACHES, ENFORCEMENT AND LIABILITY. (7.5%) (K1, K12, S1, S9)

9.1 Explain the obligation and requirements surrounding the reporting of personal data breaches (UK GDPR Articles 33 and 34).

Indicative content

a. Obligation and requirements to the ICO.
b. Obligation and requirements to the data subject.

Guidance

Candidate should be aware of all breach reporting requirements notably when it is necessary to notify the ICO and the data subject. They should also understand timescales for reporting and the documentation required.

9.2 Identify the powers of the ICO that can be imposed as a result of a data protection breach or data protection complaint (Article 58 UK GDPR).

Indicative content

a. Investigative Powers.
b. Information Notices.
c. Consensual Audits.
d. Assessment Notices.
e. Corrective Measures.
f. Warnings.
g. Reprimands.
h. Enforcement Notices.
i. Penalty Notices.

Guidance

Explain the varying powers of the ICO which may impact on controllers who have been responsible for data breaches.

9.3 Describe liabilities.

Indicative content

a. Compensation.
b. Liability between controller and processor.
c. Awareness of the existence of criminal liability regarding breaches under the Data Protection Act 2018.

Guidance

Candidates should be aware of the liability regime regarding the UK GDPR and the DPA.

SYLLABUS

10. PRIVACY AND ELECTRONIC COMMUNICATIONS (EC DIRECTIVE) REGULATIONS (PECR) 2003 AND SUBSEQUENT AMENDMENTS. (5%) (K1, K12, S7, S8, S9)

10.1 Identify the relationship between the UK GDPR, Data Protection Act 2018 and PECR in respect of marketing. (Email phone, SMS, in-app messaging, push notifications).

Indicative content

a. Objective and broad scope (email, phone, SMS, in-app messaging, push notifications).
b. Provisions relating to electronic marketing communications.
c. Role of the ICO in relation to PECR.
d. Investigating complaints.
e. Penalties for breaches of PECR marketing requirements.

Guidance

Candidates should have a broad understanding of the marketing regulations outlined in PECR including what constitutes a marketing PECR breach, the ICO's stance on PECR breaches and subsequent penalties.

EXAMINATION FORMAT

This award is assessed by completing an invigilated online exam that candidates will only be able to access at the date and time they are registered to attend.

Adjustments and/or additional time can be requested in line with the BCS reasonable adjustments policy for candidates with a disability or other special considerations, including English as a second language.

TYPE

40 MULTIPLE CHOICE QUESTIONS

DURATION

60 MINUTES

SUPERVISED

YES

THIS EXAM WILL BE SUPERVISED

OPEN BOOK

NO

(NO MATERIALS CAN BE TAKEN INTO THE EXAMINATION ROOM)

PASSMARK

(65%)

26/40

DELIVERY

DIGITAL OR PAPER BASED

QUESTION WEIGHTING

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

- Guidance on the proportion of content allocated to each topic area.
- Guidance on the proportion of questions in the exam.

Syllabus Area

1	An Introduction to the History of Data Protection in the U.K. (6%)
2	Principles of Data Protection and Applicable Terminology. (15%)
3	Lawful bases for processing Personal Data. (10%)
4	Accountability Principle (21.5%)
5	Obligations of Controllers, Joint Controllers and Data Processors. (7.5%)
6	International Data Transfers under EU and UK GDPR. (7.5%)
7	Data Subject Rights. (12.5%)
8	Independent Supervisory Authorities (ISAs) and the Information Commissioner's Office (ICO). (7.5%)
9	Breaches, Enforcement and Liability (7.5%)
10	Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003 and subsequent amendments. (5%)

RECOMMENDED READING

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

OTHER BACKGROUND MATERIALS

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 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

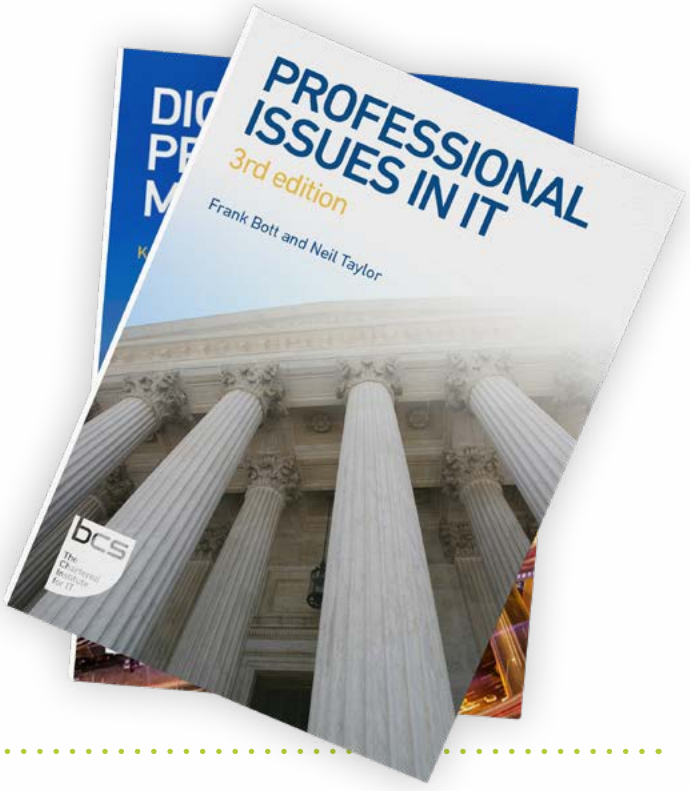
U.K. ICO detailed guidance on subject access requests https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/

UK ICO Guide to DPIAs https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/

UK ICO Accountability Framework https://ico.org.uk/for-organisations/accountability-framework/

USING BCS BOOKS

Accredited Training Organisations may include excerpts from BCS books in the course materials. If you wish to use quotes from the books, you will need a license from BCS. To request an appointment, please get in touch with the Head of Publishing at BCS outlining, the material you wish to copy and the use to which it will be put.



DOCUMENT 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 3.6 January 2023	**Document created based on syllabus refresh for v3.6 and has been transposed onto the new syllabus format with indicative content and gudiance.** **Other changes include:** **- LO 1.2 is the old LO 1.3 (v3.5).** **- LO2.1 reorded and expanded to include genetic data, pseudonymisation and anonymisation.** **- LO2.2.7 removed. This is already covered in key topic 4.** **- LO3.2 Added new sub LO to indicative content 'Identify which of the above also require additional conditions and safeguards as part of Schedule 1 of the DPA 2018.'** **- Topic 4 renamed from the old 'Governance and accountability of data protection within organisations' to Accountability Principle but content the same.** **- LO 4.9 name has been simplified with further detail added to guidance.** **- LO 6.1 name changed to focus on UK GDPR - sub objectives changed to reflect this.** **- Topic 9, slight change to wording of LOs in topic 9 'EU GDPR' and 'To an ISA' (in sub LO 9.1.1) removed. LO9.2 amended to reflect powers of the ICO. Sub LOs amended to reflect this.** **- LO 10.1 - wording changed to reinforce that this only relates to marketing.**
V3.5 July 2022	**Syllabus has been mapped to the KSBs in the Level 4 Data Protection and Information Governance Practitioner apprenticeship. Introduction has been amended to remove mention of previous update and to highlight that the syllabus has been mapped to the KSBs in the L4 Data Protection and Information Governance Practitioner apprenticeship. 1.1.5 has been removed. 4.9 has been added. 4.3has been amended. Weightings adjusted accordingly. Two items have been added to the reading list: 'UK ICO Guide to DPIAs' and 'UK ICO Accountability Framework'.**
V3.4 December 2021	**Syllabus amended to reflect changes in legislationaffectingthe introduction, key topics 1 and 10 and recommended reading.**
V3.3 July 2021	**Syllabus amended to reflect Brexit changes enshrined in legislation and current cases.**
Version 3.1 August 2020.	**Corrected trainer requirements.**

For further information please contact:
BCS
The Chartered Institute for IT
3 Newbridge Square
Swindon
SN1 1BY
T +44 (0)1793 417 417
www.bcs.org
© 2023 Reserved. BCS, The Chartered Institute for IT
All rights reserved. No part of this material protected by this copyright may be reproduced or utilised in any form, or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without prior authorisation and credit to BCS, The Chartered Institute for IT.
Although BCS, The Chartered Institute for IT has used reasonable endeavours in compiling the document it does not guarantee nor shall it be responsible for reliance upon the contents of the document and shall not be liable for any false, inaccurate or incomplete information. Any reliance placed upon the contents by the reader is at the reader's sole risk and BCS, The Chartered Institute for IT shall not be liable for any consequences of such reliance.