2023 | JUNE V9.7

BCS PRACTITIONER CERTIFICATE
IN DATA PROTECTION

SYLLABUS

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

CONTENTS

INTRODUCTION 03

LEARNING OUTCOMES 03

CERTIFICATION 04

TRAINER CRITERIA 04

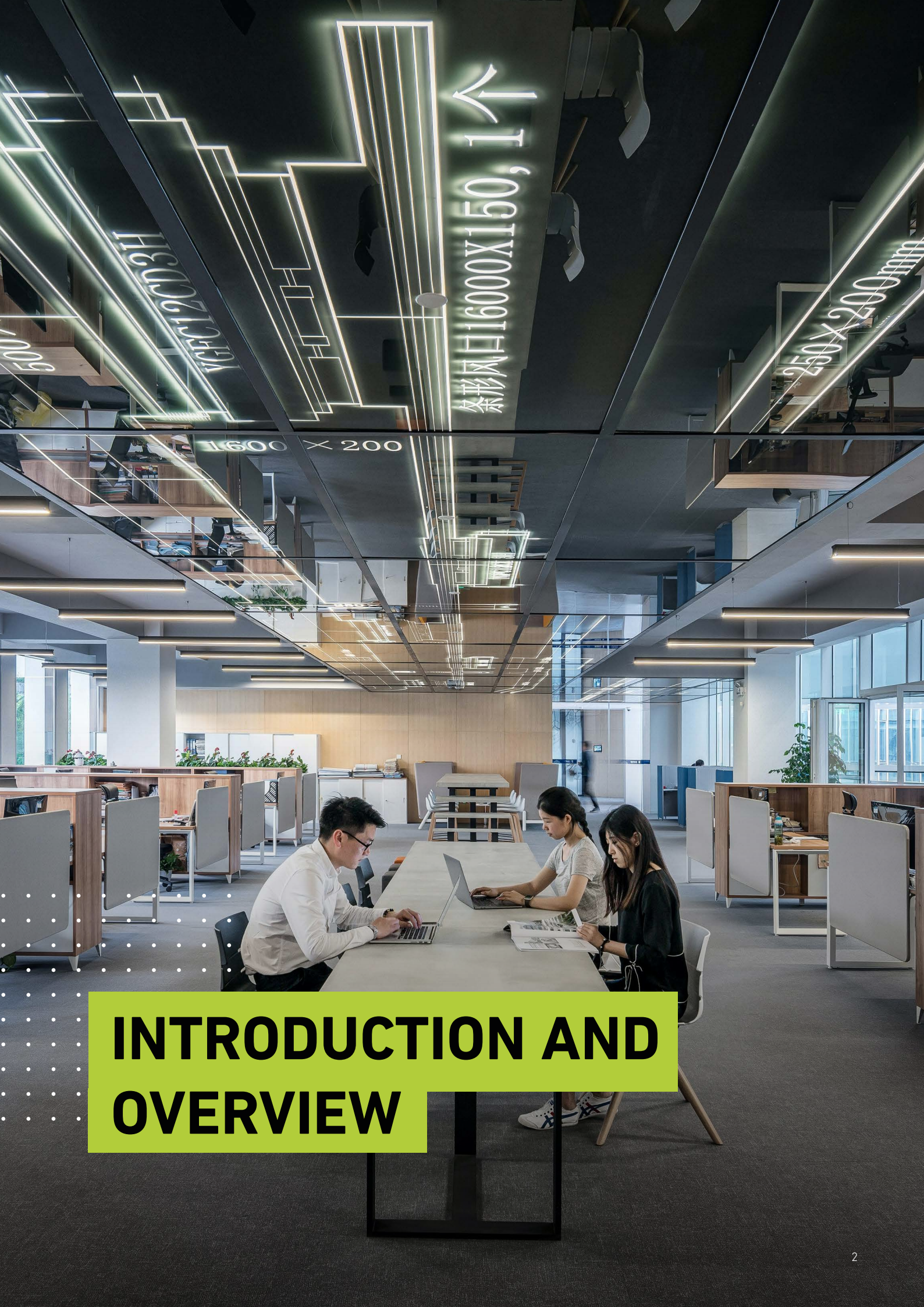
SYLLABUS 05

EXAMINATION FORMAT 29

QUESTION WEIGHTING 30

RECOMMENDED READING 31

DOCUMENT CHANGE HISTORY 33



INTRODUCTION AND OVERVIEW

INTRODUCTION

Knowledge of UK data protection law, incorporating the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 18), 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 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. It also includes the two adequacy decisions published 28 June 2021 by the EU Commission in respect of the UK regarding transfers under the EU GDPR; and to transfers under the Law Enforcement Directive (LED).

LEARNING OUTCOMES

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

- Context of data protection legislation.
- Principles of data protection and applicable terminology.
- Lawful basis for processing of personal data.
- Accountability principle.
- Obligations of Controllers, Joint Controllers and Data Processors.
- International Data Transfers under EU and UK GDPR.
- Data subject rights.
- The role of independent supervisory authorities (ISAs) and the ICO.
- Breaches, enforcement and liability.
- Processing of personal data in relation to children.
- Specific provisions in data protection legislation of particular relevance to public authorities. (7.5%).
- Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003 and subsequent amendments to 2021.
- Application of data protection legislation in key areas of industry.
- AI and the processing of personal data.

CERTIFICATION SUITABILITY AND OVERVIEW

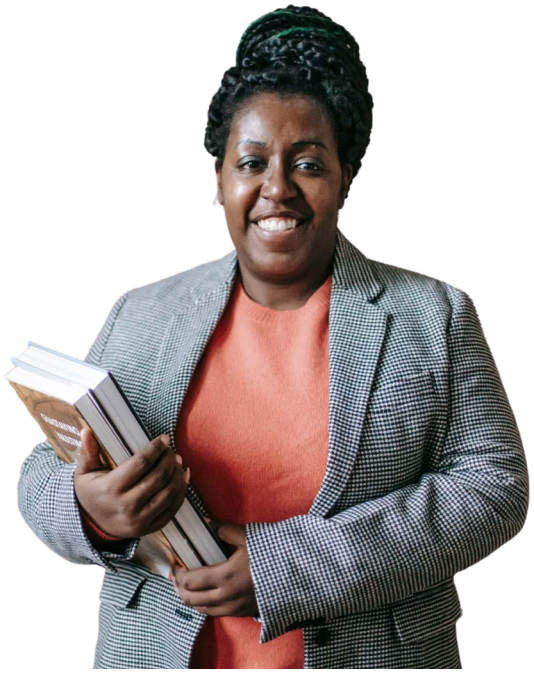
This certification is aimed at those candidates who have, or wish to have, some responsibility for data protection within an organisation and need to understand the changes that the EU GDPR, the UK GDPR and the UK Data Protection Act 2018 have brought to data protection in practice and what needs to be done to steer their organisations towards compliance. 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.

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 UK & EU GDPR in particular. 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

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	GUIDED LEARNING HOURS	INDEPENDENT LEARNING	ASSESSMENT TIME
34 hours	22.5 hours	10 hours	90 minutes



TRAINER CRITERIA

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

- The BCS Practitioner Certificate in Data Protection.
- 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 EU & UK GDPR and have a comprehensive understanding of its impact upon the practical implementation of data protection compliance.

SYLLABUS

SYLLABUS

1. CONTEXT OF DATA PROTECTION LEGISLATION. (7.5%)

1.1 Explain the concepts of data protection and privacy.

Indicative content

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

Guidance

Candidates should be able to define the terms 'data protection' and 'privacy' and explain the differences between them. What do data protection and privacy mean? Why is data protection important?

1.2 Describe the history of data protection in the UK.

Indicative content

a. United Nations Universal Declaration on Human Rights.
b. European Convention on Human Rights and Fundamental Freedoms (ECHR), (Article 8 – Respect for privacy and family life, Article 10 – Freedom of Expression).
c. Council of Europe Convention 108, 1981, its implementation by the Data Protection Act 1984, and updating of Convention 108.
d. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013 Data Protection Directive 95/46/EC.
e. Human Rights Act 1998.
f. Data Protection Act 1998.
g. Privacy and Electronic Communications Regulation 2003 and subsequent amendments to 2021.
h. General Data Protection Regulation 2016/679.
i. UK Data Protection Act 2018. The purpose of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.
j. UK GDPR.
k. Future legislative changes – Data Protection & Digital Information (No.2 Bill).

Guidance

Candidates should be able to describe the evolution of the legislative framework for data protection in the European Union and the UK but are not expected to have a detailed knowledge of the content of the above, or the chronological order.

1.3 Describe the territorial scope and jurisdiction of GDPR.

Indicative content

a. Territorial scope and jurisdiction of EU GDPR.
b. Territorial scope and jurisdiction of UK GDPR.
c. Co-operation between independent supervisory authorities.

Guidance

Candidates should be able to describe how the wider territorial scope and jurisdiction of the EU GDPR and UK GDPR impacts on the processing of personal data by global organisations.

1.4 When a representative of the controller is needed.

Indicative content

a. European Representative.
b. UK Representative.

Guidance

Candidates should be able to outline the obligations for controllers in relation to pointing European and UK representatives.

SYLLABUS

2. PRINCIPLES OF DATA PROTECTION AND APPLICABLE TERMINOLOGY. (5%)

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 Data Protection Act 2018).
e. Processing of personal data – including scope of processing (Article 2 UK GDPR).
f. Pseudonymisation and anonymisation.
g. Purely Personal and Household purposes.
h. Profiling.
i. Filing system.
j. Data subject.
k. Consent.
l. Controller.
m. Processor.
n. Recipients and third parties.

Guidance

The candidate should be able to demonstrate knowledge and understanding of all the key definitions relating to personal data under UK GDPR. Candidates should be able to explain how the terms pseudonymisation and anonymisation relate to the processing of personal data.

2.2 Demonstrate how the following UK GDPR principles regulate the processing of personal data.

Indicative content

a. Lawfulness, Fairness and Transparency - Article 5 (1)(a).
b. Purpose Limitation - Article 5 (1)(b) including compatibility.
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 define and explain the UK GDPR personal data processing principles. They should also be able to explain the considerations when processing existing personal data for a new purpose.

SYLLABUS

3. LAWFUL BASES FOR PROCESSING PERSONAL DATA. (5%)

3.1 Illustrate the lawful bases 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

Candidates should be able to explain the legitimate bases for processing personal data and explain when these legitimate bases are applicable.

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

Indicative content

a. Conditions for processing special category data.
b. Special category data, the additional conditions required and safeguards (Schedule 1 of the Data Protection Act (DPA) 2018).
c. Substantial public interest conditions (Part 2, Schedule 1 Data Protection Act (DPA) 2018).
d. Appropritate Policy document.

Guidance

Candidates should be able to identify the ten conditions for processing special category data required in Article 9 of the UK GDPR and which five require additional conditions and safeguards as set out in the Data Protection Act 2018. They should understand when an Appropriate Policy document is required. Candidates should also have an awareness of the substantial public interest conditions but there is no requirement to know these in detail.

3.3 Explain the rules for processing criminal offence data.

Indicative content

a. The definition of criminal offence data.
b. The rules for processing criminal offence data including reference to Schedule 1 Part 3.

Guidance

Candidates should be able to describe the range of information about offenders or suspected offenders which is classed as criminal offence data including criminal activity, allegations, investigations etc. They should also be able to explain the processing rules for criminal offence data and the restrictions on maintaining registers of criminal convictions. Candidates should explain how the risks associated with criminal offence data affect other data processing obligations.

SYLLABUS

4. ACCOUNTABILITY PRINCIPLE. (20%)

4.1 Identify the accountability and data governance obligation (Article 5 (2) Article 24).

Indicative content

a. The Accountability obligation under UK GDPR: including responsibility for compliance and demonstration of compliance.
b. The requirements and purpose of a privacy management framework to meet the accountability obligation.

Guidance

Candidates should be able to explain why a controller needs to take responsibility for compliance with the UK GDPR, and the key measures that can be implemented to demonstrate compliance such as policies, training, reporting structures, and risk assessment and evaluation processes.

4.2 Describe the purpose of a Data Protection Impact Assessment (DPIA) and when risks arising from one may need prior consultation with the supervisory authority/ICO (Article 36).

Indicative content

a. What a DPIA is and its purpose.
b. When a DPIA is required under UK GDPR.
c. What should be taken into consideration when assessing risks identified through DPIAs.
d. When it is a mandatory requirement to consult the ICO following a DPIA.

Guidance

Candidates should be able to explain what a DPIA is, when it is needed, the difference between the legal requirement to carry out a DPIA (due to the nature of the data being processed) and when it is good practice, how risks should be evaluated and when it is a requirement to consult the ICO.

4.3 Demonstrate the process of conducting a DPIA (Article 35).

Indicative content

a. How a DPIA is undertaken and what needs to be documented.
b. The process for evaluating risks and considering mitigations.
c. Identify who else should be consulted when completing a DPIA.

Guidance

Candidates should be able to identify the need to conduct a DPIA prior to high-risk processing and the requirement to document within the DPIA the nature, scope, context and purposes of processing. Candidates should recognise the need to consult with stakeholders, the Data Protection Officer if one is in place and potentially data processors. Candidates should demonstrate knowledge of how high risks should be evaluated and recorded and the need to identify and suggest the implementation of mitigations.

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

Indicative content

a. Definition and purpose of a RoPA.
b. Information to be included in a RoPA.

Guidance

The candidate should be able to explain what a RoPA is and why it is required to assist a controller in meeting their Accountability obligations. The candidate should be able to describe the information that needs to be documented in a RoPA as outlined in UK GDPR. They should describe the obligations of Processors to create and maintain a RoPA on behalf of a Controller.

SYLLABUS

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

Indicative content

a. Describe what a privacy notice is, in respect of the UK GDPR Transparency principle.
b. Outline what information needs to be provided to data subjects with regards to their personal data when it is collected (i) directly from the individual and (ii) collected about the individual from other sources.

Guidance

The candidate should be able to explain what a privacy notice is, what information it should contain and how the individual is made aware of when their personal data is collected and how it is used. The candidate should also be aware of how controllers can present their privacy notices to ensure they fulfil the transparency principle and make it easy and simple for people to access and understand.

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

Indicative content

a. Data protection by design.
b. Data protection by default.
c. Responsibilities for compliance.

Guidance

The candidate should be able to explain the concepts of data protection by design and default and the requirements for this under UK GDPR. The candidate should be able to describe how controllers can undertake this in practice, who is responsible for compliance and how it links in with the DPIA process.

4.7 Identify suitable information security measures (Article 32).

Indicative content

a. UK GDPR and the importance of information security.
b. Organisational measures.
c. Technical measures.
d. Data processors and information security.

Guidance

The candidate should be able to explain what security measures 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).

Indicative content

a. Outline the requirement to appoint a DPO.
b. Describe the position and remit of an appointed DPO.
c. Identify the tasks of a DPO.

Guidance

Candidates should be able to describe the criteria for appointing a DPO, the remit and purpose of the position and the key tasks that the role requires the DPO to undertake.

4.9 Explain the scope of the DPO role in monitoring compliance and managing risks through a Privacy Management programme (Article 39 1.b).

Indicative content

a. Role of the DPO in monitoring compliance.
b. Approach of the DPO in assessing, evaluating and measuring risks.

Guidance

The candidate should be aware of the role of the DPO in identifying, evaluating and measuring risks connected with data processing, and the approach to monitoring compliance within a controller organisation. The candidate should be aware of the remit of the DPO in respect to accountability for compliance (they are not accountable) and the required action if advice from a DPO is not followed.

SYLLABUS

5. OBLIGATIONS OF CONTROLLERS, JOINT CONTROLLERS AND DATA PROCESSORS. (10%)

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

Indicative content

a. The obligations of controllers.
b. The obligations of processors.

Guidance

The candidate should be able to identify and explain the distinctions between the responsibilities and obligations of controllers and processors under UK GDPR, when processing personal data. These include record keeping, responsibilities for security and compliance with international data transfer requirements.

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

Indicative content

a. Joint controllers.

Guidance

Candidate should be able to define what a joint controller is and their roles and responsibilities in respect of data processing. Candidates should also identify what impact joint controllers may have on the data subject when processing their personal data.

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

Indicative content

a. Processing under the authority of a controller or processor.

Guidance

Candidates should be able to explain the requirements concerning the processing of personal data on the instructions of the controller.

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

Indicative content

a. What a data processing contract/agreement is and when it is required.
b. What should be included in a data processing contract/agreement.
c. The arrangements required for sub-processors.

Guidance

Candidates should be able to explain the legal agreements required when a controller uses a processor to process personal data on their behalf and the UK GDPR stipulations around what needs to be included in such an agreement. The candidate should also be aware of the arrangements that are required if a processor engages a sub-processor.

SYLLABUS

6. INTERNATIONAL DATA TRANSFERS UNDER EU AND UK GDPR. (2.5%)

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

Indicative content

a. The impact of data transfers to and from the European Economic Area as a result of Brexit.
b. Post-Brexit adequacy regarding transfers under EU GDPR.
c. Post-Brexit adequacy regarding transfers under the Law Enforcement Directive.
d. Demonstrate a knowledge of the concept of "restricted transfers" and the mechanisms/ safeguards for ensuring these are undertaken lawfully.

Guidance

Candidates should explain the importance of ensuring the free flow of personal data against the considerations required when personal data is transferred to a third country that does not have adequate protection in place.

They should be able to explain the mechanisms in place which permit lawful international transfers. Demonstrate the implications of data transfers from the UK to Europe and vice versa since Brexit.

SYLLABUS

7. DATA SUBJECT RIGHTS. (5%)

7.1 Demonstrate a detailed knowledge of the key rights granted to individuals (Articles 12 to 17 and 21 to 22).

Indicative content

a. Being informed (transparency), including of further processing compatibility (Article 13 and Article 14).
b. Subject access (Article 15).
c. Prohibition against enforced subject access requests (Section 184 of DPA 18).
d. Void contractual terms relating to health records (Section 185 of DPA 18).
e. Rectification (Article 16).
f. Erasure (Right to be forgotten) (Article 17).
g. Objection (Article 21).
h. Automated individual decision making and profiling (Article 22).

Guidance

The candidate should be able to explain in detail the different rights that the UK GDPR grants to individuals whose personal data is processed and how controllers should ensure that they can fulfil requests from data subjects in respect of these rights.

7.2 Express awareness of the following rights in addition to the above.

Indicative content

a. Restriction of processing (Article 18).
b. Obligation to notify the rectification, erasure or restriction to recipients and the data subject (Article 19).
c. Portability (Article 20).

Guidance

Candidates should have an awareness of these additional rights but are not expected to know them in detail.

7.3 Describe the restrictions and exemptions that may affect data subject rights.

Indicative content

a. Restrictions (Article 23).
b. Exemptions (Schedule 2 - Parts 1 to 4 of Data Protection Act 2018).

Guidance

Candidates should have an awareness of the restrictions and exemptions that may impact on an individual having their rights fulfilled under UK GDPR.

7.4 Explain the fundamental rights of information requests.

Indicative content

a. Freedom of Information rights (FOI).
b. Environmental Information Regulation (EIR).

Guidance

The candidate should explain what these rights and regulations are and their purpose. They should explain how requests can be made, what they are expected to do in response to requests and how long they have to respond. The candidate should consider how these requests can be implemented and any exemptions to the FOI and EIR. They should consider the public interest test and if it is in the public interest to know this information.

SYLLABUS

8. THE ROLE OF INDEPENDENT SUPERVISORY AUTHORITIES (ISAS) AND THE ICO. (7.5%)

8.1 Explain the role and importance of supervisory authorities.

Indicative content

a. Independence.
b. Competence and powers (EU GDPR Article 58 (1) & 58 (2)).
c. Consistency.

Guidance

Candidates should be able to explain the role of ISAs, the importance of their independence and an overview of their roles/powers. They should also be aware of mechanisms to support cooperation and consistency between ISAs.

They should be able to describe the Role of the European Data Protection Board (EDBP) however they will not be expected to list the individual tasks in Article 70 EU GDPR. Whilst the EDPB is no longer binding under the UK regime, under ICO guidance, it is recommended that those studying GDPR retain knowledge of useful EU legislation and terms.

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

Indicative content

a. As a regulator.
b. Investigation and correction (Article 58).
c. Enforcement of regulations.
d. Data protection audits by the ICO.
e. As a body that creates guidance and codes of practice.
f. Promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing.
g. Promotion of approved privacy seals, certification schemes and availability of commonly used standards.
h. Advice and reporting to Parliament, the UK Government and other bodies.
i. Data Protection Fees.

Guidance

The candidate should demonstrate detailed knowledge of the ICO's role as the UK Data Protection Regulator and their tasks and responsibilities. Candidates should be aware of the impact of the ICO on controllers with respect to enforcement activity, audits, guidance and codes of practice. They should be familiar with the data protection fees that the ICO requires data controllers to pay which replaces the previous regime of registration.

SYLLABUS

9. BREACHES, ENFORCEMENT AND LIABILITY (12.5%)

9.1 Explain what constitutes a personal data breach and the information required for reporting.

Indicative content

a. Identifying a data protection breach.
b. Assessing a data protection breach.

Guidance

The candidate should be able to define a data protection breach and be aware of the varying kinds of incidents that may constitute a breach. Theys should recognise and explain the process for risk-assessing data breaches to ensure that they are able to gather all necessary information required for reporting if required.

9.2 Explain when the obligations arise to report breaches of personal data (Articles 33 and 34 UK GDPR).

Indicative content

a. To the ICO.
b. Data Subject.
c. To a controller (if a data processor).

Guidance

The candidate should explain the criteria which determines whether a data breach needs formal notification to the ICO and the data subject. They should be aware of reporting timescales and the necessary documentation that needs to be provided. Candidates also need to understand the role that processors have if a breach occurs.

9.3 Explain how a data protection complaint should be handled (Article 57 (1)(f)).

Indicative content

a. What constitutes a data protection complaint.
b. Role of the controller following a data protection complaint.
c. Role of the ICO following a data protection complaint.

Guidance

The candidate should be able to explain an individual's right to raise a data protection complaint about a controller concerning how their personal data has been handled. They should be able to describe what constitutes a data protection complaint and the process ensuring a complaint is handled appropriately.

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

Indicative content	Guidance
a. Information notices and assessments (Sections 145 and 146 Data Protection Act 2018). b. Reprimands. c. Enforcement notices (Section 149 Data Protection Act 2018). d. Administrative fines and their levels (Article 83). e. Tier 1 fines (up to 2% (£8.7m under the UK GDPR). f. Tier 2 fines (up to 4% (£17.5m under the UK GDPR). g. Availability of multiple tiers of fines.	The candidate should be able to explain the differing sanctions and penalties that can be imposed on controllers as a result of upheld data breaches or complaints. The candidate should be able to identify what level of fines are applied to different breaches.

9.5 Describe the following liabilities:

Indicative content	Guidance
a. Compensation. b. Liability between controller and processor. c. Awareness of the existence of criminal liability regarding breaches under the Data Protection Act 2018. d. Other legislation to be considered.	The candidate should be able to explain the liabilities of controllers and processors in respect to data protection breaches and claims from individuals.

9.6 Identify the role of tribunal and judicial courts.

Indicative content	Guidance
a. Appeals against decisions of the ICO. b. Adjudication and enforcement of legal claims for data protection breaches.	The candidate should understand the way courts and tribunals manage appeals and legal claims.

SYLLABUS

10. PROCESSING OF PERSONAL DATA IN RELATION TO CHILDREN. (2.5%)

10.1 Explain how data protection legislation applies to children.

Indicative content

a. Explain the differences between the definitions of "child" within the UK GDPR (Article 8) and EU GDPR (Article 8).
b. Describe the reasons outlined in Recital 38 of the UK GDPR as to why children's data requires special protection when being processed.
c. Explain the concept of erasure (and the right to be forgotten) where it relates to children.
d. Explain what Information Society Services means.
e. Age-Appropriate Design – a code of practice for online services 2021 (as published by the ICO under Section 123) (Scope and awareness of principles).

Guidance

The candidate should be able to explain the additional data protection requirements that should be in place to protect the personal data of children. This includes additional security measures on systems, identifying an appropriate lawful basis for data processing and if relying on consent when offering an online service to a child, limiting this to children aged 13 and over, when in the UK. Further protection must be implemented when using children's data for marketing purposes or creating profiles.

SYLLABUS

11. SPECIFIC PROVISIONS IN DATA PROTECTION LEGISLATION OF PARTICULAR RELEVANCE TO PUBLIC AUTHORITIES. (7.5%)

11.1 Define the meanings of public authority and public body and how it relates to both Data Protection Act 2018 and the UK GDPR (Section 7 of Data Protection Act 2018).

Indicative content

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

Guidance

Candidates should be able to explain the definitions of public authority and public body and how it relates to the processing of personal data with particular focus on the lawfulness of processing definitions in the Data Protection Act 2018 and UK GDPR.

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

Indicative content

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

Guidance

The candidate should be aware of the requirements outlined in the UK GDPR regarding a DPO for public authorities.

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

Indicative content

a. Health data.
b. Social work data.
c. Education data..
d. Child abuse data.

Guidance

Candidates are expected to have an awareness of the existence of the exemptions, but they will not be expected to detail the individual exemptions.

SYLLABUS

12. PRIVACY AND ELECTRONIC COMMUNICATIONS (EC DIRECTIVE) REGULATIONS (PECR) 2003 AND SUBSEQUENT AMENDMENTS TO 2021. (5%)

12.1 Explain the relationship between PECR and the GDPR, including PECR's objectives and broad scope.

Indicative content

a. Objective and broad scope (email, phone, SMS, in-app messaging, push notifications).
b. Provisions relating to electronic marketing communications (excluding fax).
c. Role of the Information Commissioner's Office (ICO) in relation to PECR.
d. Investigating complaints.
e. Issuing codes of practice.
f. Penalties for breaches of PECR.
g. Application to service providers as outlined under Article 95 of UK GDPR.

Guidance

Candidates should be able to describe the relationship between PECR and the UK GDPR and the key aspects of the Regulations including: marketing permissions, the privacy of customers who use communications networks or services in relation to traffic or location data, the security of public communications services and cookies (see more in 13.3).

Candidates should also explain the role of the ICO in relation to PECR, notably with regard to penalties for breaches of PECR.

SYLLABUS

13. APPLICATION OF DATA PROTECTION LEGISLATION IN KEY AREAS OF INDUSTRY. (10%)

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

Indicative content

a. Employment Practices Code.
b. Impact on data protection legislation.

Guidance

The candidate will be aware of the Employment Practices Code, the Information Commissioner's Office's consultation in January 2023 and ongoing changes.

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

Indicative content

a. Types of video surveillance and how it is impacted by data protection law.

Guidance

The candidate should be aware of the Information Commissioner's Office's guidance on video surveillance e.g. CCTV surveillance, automatic number plate recognition, facial recognition technology, and smart devices such as video surveillance doorbells.

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

Indicative content

a. Cookies and similar digital technologies.
b. Rules on using cookies and similar digital technologies.
c. Relationship between Privacy and Electronic Communications Regulation (PECR) 2003 and UK GDPR cookie requirements.

Guidance

The candidate should be able to define what constitutes a cookie or similar digital technology and have awareness of the rules around using these concerning the impact on data protection. They should demonstrate awareness of the overlap between the cookie requirements in UK GDPR and PECR.

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

Indicative content

a. Data sharing considerations as outlined under the Data Sharing Code of Practice.
b. Ensuring compliance with data protection legislation when sharing data.

Guidance

The candidate should be able to demonstrate knowledge of the Data Sharing code of practice and explain how these requirements are governed by data protection law.

SYLLABUS

14. AI AND THE PROCESSING OF PERSONAL DATA. (5%)

14.1 Analyse the benefits versus the risks of AI for individuals and organisations.

Indicative content

a. What is meant by AI.
b. The impact on individuals and organisations.

Guidance

The candidate should explain what AI means and the benefits and risks of AI to individuals and organisations. They should explain the importance of adopting a risk-based approach when utilising AI and how this should be embedded into organisational governance.

14.2 Analyse the impact of AI on the principles and concepts of data protection.

Indicative content

a. Lawfulness.
b. Fairness.
c. Transparency.
d. Data minimisation.
e. Security.
f. Controller/Processor obligations.
g. Individual rights.

Guidance

The candidate should understand the impact AI has on key areas of data protection.

14.3 Explain the process of completing a Data Protection Impact Assessment (DPIA) where AI is used.

Indicative content

a. How the use of AI impacts the process for completing a DPIA and what needs to be recorded.

Guidance

The candidate should outline what needs to be considered when a Data Protection Impact Assessment is completed for AI.

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

90 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 Context of data protection legislation. (7.5%)

2 Principles of Data Protection and Applicable Terminology. (5%)

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

4 Accountability Principle. (15%)

5 Obligations of Controllers, Joint Controllers and Data Processors. (10%)

6 International Data Transfers under EU and UK GDPR. (2.5%)

7 Data Subject Rights. (5%)

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

9 Breaches, Enforcement and Liability (12.5%)

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

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

12 Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003 and subsequent amendments to 2021. (5%)

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

14 AI and the Processing of Personal Data. (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

Privacy and Electronic Communications (EC Directive) Regulations 2003
https://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

UK ICO Guidance on AI and data protection
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

UK ICO Guidance on AI and data protection toolkit
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/

OTHER BACKGROUND MATERIALS

U.K. ICO Guide to Data Protection (GDPR)
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

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/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/

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 "Age Appropriate Design – a code of practice for online services"
https://ico.org.uk/media/about-the-ico/documents/2618093/code-of-practice-dpa-2018-age-appropriate-design-code_v_2_1.pdf

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

U.K. ICO update report on edtech 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 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/

U.K. ICO Overview – Data Protection and the EU https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/#now

U.K. ICO Children https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/children/

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

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
V9.7 June 2023	**Syllabus amended to include:** **- Indicative Content (k) added. 'Future legislative changes – Data Protection digital information.' Showing changes that would be made by the data protection and digital information bill.** **- New LO 7.4: Explain the fundamental rights of information requests. Added to further align the Foundation and Practitioner certificates with the knowledge, skills and behaviours in the Data Protection and Information Governance Practitioner (L4) standard.** **-New Topic 14: AI and the Processing of Personal Data. Included due to the updated guidance on AI and data protection from the ICO:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/
V9.6 January 2023	**Syllabus transferred to new template including indicative content and guidance in line with other BCS certifications. Syllabus amended and updated to reflect current status of data protection legislation.**
V9.5 July 2022	**Alterations made in line with initial post-Brexit changes to compliance with EU/UK GDPR.**
V9.4 December 2021	**Syllabus amended to reflect changes to legislation affecting the introduction, key topics 1, 10, 12 and recommended reading.**
V9.3 July 2021	**Syllabus amended to reflect Brexit changes enshrined in legislation and current cases.**
V9.1 August 2020	**Trainer criteria updated.**
V9.0 June 2020	**Syllabus amended and updated to reflect current status of data protection legislation**
V8.4 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**

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