BCS Foundation Certificate in Data Protection v3.9

Sample Paper

Record your surname / last / family name and initials on the answer sheet.

Sample paper consists of 40 multiple-choice questions.

Multiple choice questions allow only one correct answer to be selected for 1 mark.

1 mark awarded to each question. There are no trick questions.

A number of possible answers are given for each question, indicated by either **A B C or D**.

Your answers should be clearly indicated on the answer sheet.

Pass mark: 26/40
Time allowed: 60 minutes

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

1 Which piece of legislation created a unified approach to data protection within Europe?

A Data Protection Act 1984.
B Privacy and Electronic Communications Regulations (PECR).
C General Data Protection Regulation.
D Law enforcement directive.

2 In which of the following scenarios would the organisation **not** be subject to UK GDPR?

A A marketing firm based in France with clients in London.
B A toy shop based in Singapore selling toys to French citizens.
C A British high-street fashion brand importing clothes from China.
D An English local council running a healthy eating campaign.

3 Which of the following is **not** special category personal data?

A Personal data revealing an individual's political opinions.
B Personal data revealing an individual's criminal convictions.
C Personal data revealing an individual's religious belief.
D Personal data revealing an individual's sexual orientation.

4 Which of the following is special category data?

A Health data.
B Date of birth.
C Job title.
D Bank account number.

5 Which definition does the following quote relate to?

"Any information relating to an identified or identifiable natural person ('data subject')."

A The definition of pseudonymised data.
B The definition of personal data.
C The definition of special category data.
D The definition of biometric data.

6 Which data protection principle is defined as follows?

"Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."

A Lawfulness, fairness and transparency.
B Purpose limitation.
C Data minimisation.
D Storage limitation.

7 Keeping a record of processing activity (ROPA) is mandatory in which of the following circumstances?

A Processing is one-off.
B Processing includes special categories of data.
C Processing is for household or personal reasons.
D The data controller is self-employed and has no employees.

8 Which data protection principle is partially defined as follows?

"Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."

A Lawfulness, fairness and transparency.
B Purpose limitation.
C Storage limitation.
D Data minimisation.

9 Which of the following is **not** a responsibility of the Data Protection Officer (DPO) under article 39 UK GDPR?

A To cooperate with the supervisory authority.
B To provide advice on data protection issues.
C To be a point of contact for data subjects.
D To allocate a financial budget towards data protection.

10 In which of the following scenarios could consent be relied on as a lawful basis?

A A local council is processing financial details to collect council tax.
B An employer is recording the address of the employee.
C A local cinema is sending customers a list of the upcoming film releases.
D An individual is completing an anonymous survey.

11 Which of the following statements does **not** apply to the Article 4 definition of consent under the UK GDPR?

A A data subject can withdraw their consent at any time.
B A data subject must have full information as to what they are consenting to.
C A controller must be able to demonstrate that consent has been given.
D Consent can be implied by the actions of the data subject.

12 Which of the following purposes is **not** a condition for processing special category data?

A Legitimate interests.
B Vital interests.
C Health or social care.
D Archiving, research and statistics.

13 How long does a public authority have to respond to an Environmental Information Regulation (EIR) request?

A 20 working days.
B 1 calendar month.
C 28 days.
D 72 hours.

14 According to the “accountability principle” in Article 5(2) (UK GDPR), who is responsible for “accountability”?

A The controller.
B The Data Protection Officer (DPO).
C The controller and the processor.
D The data subject.

15 Which of the following is **not** usually considered as part of a Data Protection Impact Assessment (DPIA)?

A Description of the purpose of the processing.
B Assessment of the risks to the rights of individuals.
C Consideration of how to reduce cost of the processing to the organisation.
D Consultation with relevant stakeholders.

16 When **should** a Data Protection Impact Assessment (DPIA) **first** be completed for an Artificial Intelligence (AI) system?

A Following a data breach.
B After the AI system has collected all training data.
C Before the development of the AI system begins.
D After the AI system has been in place for six months.

17 Which of the following **correctly** shows who is responsible for records of processing activities (ROPAs)?

A The controller.
B The controller and the processor.
C The supervisory authority and the controller.
D The processor.

18 Where personal data is collected directly from a data subject, when **should** the relevant information contained in an Article 13 (UK GDPR) privacy notice be provided?

A At the time the data is collected.
B Within a 'reasonable period', but at least within one month of the data being collected.
C At the time of the first communication within the data subject.
D At least at the time of the first disclosure of the data to a recipient.

19 Which of the following furthers the ‘data protection by design and default’ approach?

A Subject access requests.
B Data Protection Impact Assessments (DPIAs).
C Enforcement action.
D Information notices.

20 Which of the following is **not** one of the suitable information security measures identified by Article 32 of the UK GDPR?

A Delivering pseudonymisation and encryption.
B Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
C Ensuring the availability and access to personal data in a timely manner in the event of an incident.
D Ensuring the right to be forgotten is respected in all circumstances.

21 Which of the following statements about the role of the Data Protection Officer (DPO) is **incorrect**?

A They must be a full member of the board, authorising the processing.
B They cannot be dismissed for carrying out their responsibilities.
C They must be provided with all the necessary resources to carry out their role.
D They act as the point of contact with the supervisory authority.

22 Which of the following **correctly** describes joint controllers?

A Two or more controllers choosing the same processor.
B Where two or more individuals in a company determine the means of the processing.
C Two or more controllers appointing the same processor to process the same type of information.
D Two or more controllers jointly determining the purpose and means of processing.

23 Which of the following is **correct** of a processor?

A They act under the instruction of a controller.
B They determine the purpose and means of processing.
C They are an employee of the controller.
D They must only process pseudonymised data.

24 The local council contracts a local firm to complete repairs on resident homes. This means the contractor is which of the following?

A A processor.
B A controller.
C A joint controller.
D A data subject.

25 Which of the following countries does **not** have a UK adequacy regulation decision?

A New Zealand.
B Germany.
C Spain.
D South Africa.

26 An international car company would like to transfer customer data to the United States of America for analysis purposes, the company is certified under the Data privacy framework program. What would be the **most** appropriate option to transfer the personal data?

A Sending a reduced number of customers' details.
B Adequacy decision.
C Encryption.
D Binding Corporate Rules.

27 A privacy notice supports which of the following data subject rights?

A The right to be informed.
B The right to erasure.
C The right to rectification.
D The right to restrict processing.

28 Which of the following may be required of the data subject when they make a subject access request?

A Payment of a subject access fee.
B The reason why the data subject is making a request.
C Information to confirm the requestor's identity.
D Confirmation of how they will use the information.

29 A health authority relies on the public interest task as its lawful basis for processing.

Which of the following data subject rights will **not** apply?

A The right to be informed.
B The right of access.
C The right to withdraw consent.
D The right to rectification.

30 Which of the following is **not** a practical step an organisation can take to ensure they meet the Article 5 accountability principle when implementing Artificial Intelligence (AI) in a new system?

A Consulting with individuals likely to be affected by the processing.
B Conducting a Data Protection Impact Assessment (DPIA).
C Creating an AI policy.
D Limiting user access to information that is strictly necessary.

31 What is the definition of the "public interest test" when applying a qualified exemption under the Freedom of Information Act (FoIA)?

A Protecting any personal information.
B Determining which information the public finds most interesting.
C Weighing the potential harms of disclosure with the benefits.
D Protecting any information which could incriminate someone.

32 Which of the following is **not** an enforcement option available to the Information Commissioner's Office (ICO)?

A Monetary penalty.
B Compulsory audit.
C Enforcement notice.
D Corrections notice.

33 Which of the following statements accurately explains the appointment and the role of the Information Commissioner?

A A civil servant appointed by and answerable to government ministers.
B A state official, appointed by and answerable to the European Commission.
C An independent official, appointed by the state, reporting directly to the UK parliament.
D An independent official, appointed by and answerable only to the European Data Protection Supervisor.

34 Article 60 (EU GDPR) provides that the lead supervisory authority and the other supervisory authorities must co-operate.

Which of the following statements **best** describes this request for co-operation?

A To mutually assist or carry out a joint operation when carrying out investigations.
B To assist where another supervisory authority does not have the resources.
C To undertake an investigation solely on behalf of the lead supervisory authority.
D To solely assist other supervisory authorities in the task of gathering evidence in respect of a data controller.

35 Which of the following is **correct** of the Information Commissioner's Office's (ICO's) role in issuing codes of practice under the UK GDPR?

A The ICO can ensure a controller and a processor are legally bound to the provisions.
B The ICO can ensure all processing carried out by a controller or a processor follows the same conditions.
C The ICO sets out best practice to assist a controller or a processor in conducting their business lawfully.
D The ICO sets out the rules to ensure good business practice so that data subjects can understand their rights.

36 Which of the following statements **best** describes the circumstances in which a data breach should be reported to the Information Commissioner's Office (ICO)?

A Any data breach where there is a loss of personal data must be reported.
B Data breaches that result in a risk of adversely affecting the rights and freedoms of data subjects must be reported.
C Data breaches which break one of the data protection principles must be reported.
D Data breaches must be reported as soon as it is evident that a data subject will suffer harm and distress.

37 A large tech company has failed to advise the Information Commissioner's Office (ICO) of a high-risk data breach. What is the maximum fine they could receive as a result?

A £9.5 million or 4% of global turnover.
B £2.1 million.
C £8.7 million or 2% of global turnover.
D £6.5 million or 3% of global turnover.

38 Which of the following activities would be considered direct marketing under the Privacy and Electronic Communications Regulations (PECR) (2003)?

A A restaurant flyer posted to every home in the local area.
B A delivery confirmation text message.
C The sharing of holiday photographs through a family mailing list.
D A phone call from a company selling double glazing.

39 Which of the following courses of action can the Information Commissioner's Office (ICO) pursue for a contravention of the Computer Misuse Act?

A Civil litigation.
B Criminal litigation.
C Enforcement notice.
D Information notice.

40 Which of the following areas does Privacy and Electronic Communications Regulations (PECR) **not** cover?

A Marketing by electronic means.
B The use of cookies to track information about people.
C Security of electronic communication services.
D Security of the computer networks of public services.

End of Paper

Question	Answer	Rationale	Syllabus Sections
1	**C**	The GDPR is an EU Regulation, which means it is binding on member states across the EU.	LO1.1
2	**B**	A company based in Asia, selling goods to EU citizens outside of the UK would not be subject to UK GDPR (Article 3, EU GDPR and UK GDPR). The fashion brand would be subject to UK GDPR because they are based on the UK high street. The local council are UK-based and serving UK residents, so would be subject to UK GDPR. The marketing firm has clients in UK and therefore is subject to UK GDPR as per article 3(2).	LO1.2
3	**B**	Personal data revealing criminal convictions is not listed in Article 9 as special category data. Criminal offence data has its own category in Article 10 of the UK GDPR.	LO2.1
4	**A**	Health data is considered special category data under Article 9 GDPR.	LO2.1
5	**B**	Article 4(1) of the UK GDPR defines personal data as "Any information relating to an identified or identifiable natural person (‘data subject’)."	LO2.1
6	**C**	Article 5(1)(c) of the UK GDPR defines the data minimisation principle as follows: "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."	LO2.2
7	**B**	Under Article 30, a ROPA is required where the processing involves special category or criminal offence data. Personal and household information is exempt from needing a ROPA. If an individual is self-employed then they are unlikely to need a ROPA as the records kept would be very small in number.	LO4.4

8	**C**	The text "Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" partially defines the storage limitation principle, as per Article 5(1)(e) of the UK GDPR.	LO2.2
9	**D**	The DPO does not have a responsibility under article 39 to allocate any financial resources. This could be undertaken by any person in the company.	LO4.8
10	**C**	This is consent because it is a marketing email. The lawful basis for scenario A would be public interest task. Scenario B would be contract. Scenario D would not require consent as it is anonymous.	LO3.1
11	**D**	Article 4(11) (UK GDPR) defines 'consent' of the data subject as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Consent cannot therefore be implied from the data subject's actions.	LO3.1
12	**A**	Legitimate interests is not a condition for processing special category data under Article 9 of the UK GDPR.	LO3.2
13	**A**	EIR's must be responded to within 20 working days.	LO7.2
14	**A**	Article 5(2) (UK GDPR) states "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the other data protection principles]."	LO4.1
15	**C**	Cost reduction is not a focus of a DPIA. Describing the nature of processing, consulting with relevant stakeholders, and identifying and assessing risks to individuals are all important steps when carrying out a DPIA.	LO4.2

16	**C**	A DPIA for an AI system should be initiated early in the design and planning stages, before any personal data processing begins, to identify and mitigate privacy risks and ensure compliance with data protection regulations.	LO4.3
17	**B**	Under Article 30, both controllers and processors have responsibility for keeping up to date ROPAs.	LO4.4
18	**A**	Article 13(1) and Article 13(2) (UK GDPR) stipulate that information provided in an Article 13 Privacy Notice must be provided at the time the data is collected.	LO4.5
19	**B**	Undertaking Data Protection Impact Assessments when proposing to process any data that may be of a high risk to the rights and freedoms of individuals clearly furthers the privacy by design and default approach.	LO4.6
20	**D**	The right to be forgotten is not one of the information security measures identified by Article 32 of the UK GDPR.	LO4.7
21	**A**	The role of the Data Protection Officer must be free of conflict and report to the most senior authority. They cannot be a member of the board.	LO4.8
22	**D**	Article 26(1) of the UK GDPR states “Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers”.	LO5.1
23	**A**	A processor acts under the instruction of a controller (Article 28, Article 29) (UK GDPR).	LO5.1
24	**A**	In this scenario, the contractor would be a processor as they are acting on the instructions of the local council, who is the controller.	LO5.1
25	**D**	South Africa does not currently have adequacy.	LO6.1
26	**D**	Binding Corporate Rules is most appropriate as they are a multinational company.	LO6.1
27	**A**	A privacy notice supports the right to be informed in providing the data subject with information about the processing.	LO7.1

28	**C**	The data controller may request that identification is provided, such as a driving license or confirmation of information already held on the account. This is to ensure the information is disclosed to the correct person.	LO7.1
29	**C**	The right to withdraw consent will not apply where consent is not being relied on as a legal basis.	LO7.1
30	**D**	See: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-are-the-accountability-and-governance-implications-of-ai/	LO7.3
31	**C**	The public interest test applies to qualified exceptions where the benefits of openness and transparency should be considered against the possibility of harm.	LO7.2
32	**D**	Enforcement options available to the ICO include; a monetary penalty (fine), a compulsory audit or an enforcement notice.	LO8.1
33	**C**	The role of Information Commissioner is an independent official, appointed by the state, that reports directly to the UK parliament.	LO8.1
34	**A**	Article 60 of the EU GDPR states that “The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 (EU GDPR) and may conduct joint operations pursuant to Article 62 (EU GDPR), in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.”	LO8.1
35	**C**	In issuing codes of practice under the UK GDPR, the ICO sets out best practice to assist a controller or a processor in conducting their business lawfully.	LO8.2
36	**B**	Article 33 of the EU GDPR provides that a data breach should be reported to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. It therefore follows that any breach which results in a high risk of adversely affecting the rights and freedoms of data subjects is a reportable breach.	LO9.1

37	**C**	From the ICO website: ‘Failing to notify the ICO of a breach when required to do so can result in a heavy fine of up to £8.7 million or 2 per cent of your global turnover.’	LO9.2
38	**D**	Direct marketing is defined as "the communication (by whatever means) of advertising or marketing material which is directed to a particular individual."	LO10.1
39	**B**	The ICO can bring criminal litigation for offences under the Computer Misuse Act.	LO9.3
40	**D**	PECR does not relate to the security of computer networks of public services.	LO10.1