BCS Foundation Certificate in Data Protection

Sample Paper

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

Sample paper only 40 multiple-choice questions – 1 mark awarded to each question. Mark only one answer 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 is [26/40]

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

1 Finish the sentence:

The Privacy and Electronic Communications Regulations 2003:

A Replaced the Data Protection Act 1998.
B Were replaced by the UK GDPR and Data Protection Act 2018.
C Should be read alongside the UK GDPR where appropriate.
D Do not apply in the United Kingdom.

2 In which of the below 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 high-street fashion brand importing clothes from China.
D A 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 What does the following sentence describe?

"Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."

A Controller.
B Processor.
C Data Subject.
D Profiling.

5 What 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 Which of the following is INCORRECT in relation to the accuracy principle?

A Reasonable steps should be taken to ensure Personal Data remains correct.
B Reasonable steps should be taken to correct inaccurate Personal Data as soon as possible.
C Challenges to the accuracy of Personal Data must be dealt with as soon as is reasonably possible.
D Where there is a disagreement as to the accuracy of Personal Data, this data should be deleted.

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 an effective way for a data controller to demonstrate compliance with UK GDPR in respect of data protection training?

A Ensure that individuals only take data protection training if they are found to have done something wrong.
B Make sure all employees do the same training, so that there is a consistent message.
C Get the Data Protection Officer to approve the data protection training so they can ensure it covers the relevant points.
D Make sure that everyone's training records are completed when they have done their training so that they don't have to do it again.

10 Which of the following does **NOT** apply to the Article 6(1)(d) (UK GDPR) 'Vital Interests' lawful basis for processing?

A Applies only to life and death situations.
B Applies to the vital interests of the Data Subject.
C Applies only where another lawful basis can be identified.
D Applies to situations involving another person other than the Data Subject.

11 Of the following statements, which does **NOT** apply to the Article 6 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 Which of the following is **NOT** a valid purpose to process Special Category Data relying on the Article 9(2)(j) (UK GDPR) condition for processing?

A Archiving purposes in the public interest.
B Political purposes in the public interest.
C Historical research purposes.
D Scientific research purposes.

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

A A Controller.
B A Controller and a Data Subject.
C A Controller and a Processor.
D A Data Subject.

15 Which of the following is the CORRECT reason for carrying out a Data Protection Impact Assessment?

A Assessing the impact of a fine following a breach of data protection legislation.
B Establishing the impact of a project on the capacity of the Data Protection Officer.
C Identifying data protection risks and mitigating these where possible.
D Evaluating the impact of a breach on Data Subjects.

16 The following are elements of a Data Protection Impact Assessment (DPIA) process:

A. Mitigate the risks where possible.
B. Identify the need for a DPIA.
C. Assess the risks.
D. Identify the risks.

Rearrange so that they are in the CORRECT and logical order:

A A, C, D and B.
B D, B, A and C.
C B, D, C and A.
D C, D, B and A.

17 Which of the following is **NOT** required to keep a record of processing activity?

A Data Controller.
B Data Processor.
C Data Controller's representative.
D Data Subject.

18 Where personal data are 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.
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 is INCORRECT?

A Must be a full member of the Board authorising the processing.
B Cannot be dismissed for carrying out their responsibilities.
C Must be provided with all the necessary resources to carry out their role.
D Acts 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 Acts under the instruction of a Controller.
B Determines the purpose and means of processing.
C Is an employee of the controller.
D Must only process pseudonymised data.

24 Which of the following is **NOT** an obligation of a Controller under the UK GDPR?

A Set out a Privacy Notice.
B Act on the instruction of a Processor.
C Set appropriate data protection policies.
D Demonstrate compliance.

25 Which country below does not have an EU adequacy 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. What would be the most appropriate option to transfer the personal data?

A Sending a reduced number of customer's 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 Where a Controller is processing Personal Data because of a legal duty to do so, which of the following Data Subject Rights will **NOT** apply?

A The Right of Access.
B The Right to be Informed.
C The Right to Rectification.
D The Right to Restrict Processing.

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 below 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 which is strictly necessary.

31 What is the correct definition for "Machine Learning"?

A The ability for a computer system to carry out complex functions on a daily basis.
B The set of techniques and tools that allow computers to ‘think’ by creating mathematical algorithms based on accumulated data.
C When updates are added to a computer system.
D A series of techniques applied to the initial model after its original training.

32 Which of the following countries have **NOT** been deemed adequate by the European Commission?

A Argentina.
B India.
C New Zealand.
D Uruguay.

33 Of the following statements, which accurately explains the appointment and the role of 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 European Data Protection Supervisor.

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

Of the below statements, how is this request for co-operation **BEST** described?

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 is 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 What statement **BEST** describes the circumstances in which a data breach should be reported to the Information Commissioner's Office?

A Any data breach where there is a loss of personal data must be reported.
B Data breaches which result in a high risk of adversely affecting the rights and freedoms of data subjects.
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 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 is an example of direct marketing under Privacy and Electronic Communications Regulations?

A An email sent to an individual about an order she has placed for a pair of shoes advising her of late delivery.
B An email sent to an individual advising of a forthcoming sale.
C An email sent to all customers of a utility company about a change to terms and conditions.
D A, B, and C.

39 Which of the following courses of action can the Information Commissioner's Office 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 **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 Privacy and Electronic Communications Regulations 2003 should be read alongside the UK GDPR. The UK GDPR will apply to any personal data being collected.	LO1.1.
2	**B**	Article 3, EU GDPR and UK GDPR - answer is an Asian country selling to the EU. No mention of UK citizens. Fashion brand would be subject to UK GDPR because they are based in the UK high street. Local council would be UK based and UK residents. The marketing firm has clients in UK therefore 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**	Article 4(7) of the UK GDPR defines a Controller as the "Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."	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	**D**	Where there is a disagreement about the accuracy of personal data, it does not follow that it should be deleted. For example, where there is a legal obligation to collect and process personal data, the right to erasure does not apply.	LO2.2.
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	**C**	One of the tasks of the DPO would be to ensure that a training course contains all the necessary information to make sure people understand their responsibilities. All individuals should do training and refresher training regularly. Training should	LO4.9

Question	Answer	Rationale	Syllabus Sections
		be tailored to bespoke responsibilities for any individuals who may handle higher risk data.	
10	**C**	Recital 46 of the UK GDPR provides clarification that 'vital interests' means "an interest which is essential for the life of the data subject or that of another natural person". Article 6(1)(d) UK GDPR (Vital Interests) therefore applies only to life and death situations.	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 subjects 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	**B**	Article 9(2)(j) of the UK GDPR provides that Article 9(1) does not apply where the "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes…". Political purposes in the public interest is not therefore such a condition for processing.	LO3.2.
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**	Recital 90 states that "A data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation."	LO4.2.
16	**C**	Before processing Personal Data, it should be established whether a DPIA is required. This is the first logical step of the process identified. Having identified that a DPIA is required those risks must be identified before they can be assessed. As soon as the risks have been	LO4.3.

Question	Answer	Rationale	Syllabus Sections
		appropriately assessed, they should then be mitigated where possible.	
17	**D**	Article 30(1) of the UK GDPR requires a Controller and the Controllers representative to keep a record of processing activity. Article 30(2) of the UK GDPR requires each processor and, where applicable, the processor's representative to maintain a record of all categories of processing activities carried out on behalf of a controller. A Data Subject is the subject of the data. There are no obligations on data subjects in the UK GDPR.	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	**B**	A processor acts under the instruction of a Controller (Article 28, Article 29) (UK GDPR), a controller does not act under the instruction of a processor.	LO5.1.
25	**D**	South Africa does not currently have adequacy.	LO6.1.
26	**D**	BCR 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	**D**	The Right to Restrict Processing will not apply as the Controller is under a legal obligation to undertake the processing.	LO7.1.

Question	Answer	Rationale	Syllabus Sections
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: ICO: AI and accountability	LO7.3.
31	**B**	Machine learning involves utilising algorithm based technologies to complete complex tasks that allows computers to 'think'. ICO Definitions	LO7.3.
32	**B**	India has not received an adequacy decision.	LO6.1
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.	LO8.1.
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 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	**B**	Only B is classed as marketing.	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.