BCS Foundation Certificate in Data Protection

Specimen Paper

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

Specimen paper only 20 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 [13/20]

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

1 When did the UK GDPR become enforceable?

A 1998.

B 2003.

C 2018.

D 2016.

2 What is the purpose of Pseudonymisation?

A It makes it impossible to attribute a piece of data to a specific person without additional information.

B It mitigates the requirement for consent.

C It encrypts data so it cannot be read if accessed by hackers.

D It negates the requirement to fulfil a data subject request.

3 Which of the following is **NOT** one of the UK GDPR data protection principles?

A Data minimisation.

B Purpose limitation.

C Data encryption.

D Storage limitation.

4 A car company wants to market a new car to its existing customers.

Identify the **MOST** appropriate lawful basis for processing:

A Public interest.

B Business to business.

C Legitimate interests.

D Contract.

5 Which of the following Article 9 (UK GDPR) conditions of processing may be used to process special category data?

A Legitimate interests.

B Public health.

C Contract.

D Profiling.

6 Which **BEST** describes the purpose of a Data Protection Impact Assessment (DPIA)?

A To ensure personal data is encrypted.

B To assist in effectively tracking consent.

C To help you identify and minimise the data protection risks of a project.

D To help you decide if you can use legitimate interests as a lawful basis.

7 Article 30 of the UK GDPR states that you must:

A Respond to Data Subject Requests within 72 hours.

B Keep records of your processing activities.

C Ensure that all 3rd party processors encrypt their databases.

D Unsubscribe users after one year of inactivity.

8 Which **BEST** describes data protection by 'design and default'?

A Employing a dedicated Data Protection Officer to ensure policies are in place.

B Always using the best available security solution for any personal data.

C Deploying appropriate technical and organisational measures to meet UK GDPR principles.

D Ensuring consent is always obtained when processing personal data.

9 Which of the following statements regarding Data Protection Officers (DPOs) is **FALSE**?

A The DPO must report to the highest management level.

B A DPO may perform additional job roles.

C The DPO must be a permanent employee.

D A DPO's role has a protected status.

10 Which of the following BEST reflects Article 30 (UK GDPR) - Records of Processing?

A Controllers have sole responsibility for records of processing.

B Processors have sole responsibility for records of processing.

C Processors and controllers are both required to maintain records of processing.

D Processors, controllers and data subjects are each responsible for their own records of processing.

11 When processing personal data under the authority of the controller or processor, a processor may process data on instructions from the controller and also:

A Under Legitimate Interests.

B For business to business marketing.

C Where required to do so by Union or Member State law.

D For service messages only.

12 Which of the following describes a country which has similar data protection standards as the UK GDPR or EU GDPR and has received approval from the European Commission?

A Privacy Shield.

B Adequacy.

C Derogations.

D Compliance.

13 You are tasked with creating a company policy for handling data subject requests. elect an appropriate policy statement:

A Data subject requests must be responded to within 72 hours.

B Data subject requests must be submitted in writing to the Data Protection Officer.

C A subject access request can be refused if it is excessive.

D A subject access request can be refused if it includes financial transactions.

14 Under which circumstances may a data subject request be refused:

A Releasing the data could be damaging to the business.

B It involves disclosing personal information about other people.

C The data subject is under the age of 14.

D The data subject has refused to pay the fee.

15 What assistance does the Information Commissioner's Office offer companies in achieving and maintaining compliance with the UK GDPR?

A Conducting data protection audits for UK companies.

B Advising on appropriate wording for consent statements and privacy policies for your website.

C Providing data protection courses for the public.

D Liaising with the European Data Protection Board (EDPB) on behalf of UK companies.

16 Select the enforcement action that the Information Commissioner's Office may take in the event of a compliance breach.

A Order the company to pay compensation to the data subjects.

B Prosecute the shareholders of the company.

C Issue enforcement notices.

D Dock salaries of the company directors.

17 Under which circumstances are personal data breaches **NOT** reportable to an independent supervisory authority?

A There is minimal risk to the data subject.

B It could make the company liable to legal action by the data subject.

C The data was breached by a third party data processor.

D The company does not conduct large-scale, systematic processing of data.

18 Which of the below is **NOT** an enforcement option available to the Information Commissioner's Office?

A Penalty notice.

B Assessment notice.

C Information notice.

D Corrections notice.

19 Which of the following would definitely not be special category data?

A A mobile app which stores individuals Covid test results.

B A list of Trade Union members who work for a public sector organisation.

C A voice recording used to identify and validate people who ring into a contact centre.

D A hospital record holding the medical cause of death of an identified individual.

20 You've been asked to redesign your company's marketing strategy to ensure it is fully compliant with data protection law. The current strategy was designed before 2016 and was not created with data protection in mind so you decide to start from scratch, creating a presentation for the board outlining your requirements.

Choose the CORRECT statement below:

A Consent gained under Privacy and Electronic Communications Regulations (2003) does not have to meet UK GDPR specifications.

B Privacy and Electronic Communications Regulations (2003) applies to B2B marketing, UK GDPR does not.

C The UK GDPR replaced the Privacy and Electronic Communications Regulations (2003) in 2018.

D Electronic marketing campaigns must comply with Privacy and Electronic Communications Regulations (2003) and UK GDPR.

End of Paper

BCS Foundation Certificate in Data Protection
Answer Key and Rationale

Question	Answer	Explanation / Rationale	Syllabus Section
1	**C**	The UK GDPR became enforceable on 25 May 2018.	LO1.1
2	**A**	Pseudonymisation is a technique that replaces or removes information in a data set to render the data subject unidentifiable.	LO2.1
3	**C**	The UK GDPR Principles are: Lawfulness, fairness and transparency, Purpose limitation, Data minimisation, Accuracy, Storage limitation, Integrity and confidentiality (security), Accountability.	LO2.2
4	**C**	Legitimate interest may be used to conduct marketing ONLY in a Business to Business context.	LO3.1
5	**B**	See UK GDPR Article 9, 2 (i)	LO3.2
6	**C**	See Article 35, UK GDPR (data protection impact assessment).	LO4.2
7	**B**	See Article 30, UK GDPR.	LO4.4
8	**C**	Article 25,UK GDPR (data protection by 'design and default') data protection must be integrated, or 'baked in' to your systems.	LO4.6
9	**C**	See Article 37–39, UK GDPR.	LO4.8
10	**C**	See Article 28, UK GDPR.	LO5.1
11	**C**	See Article 29, EU GDPR and UK GDPR.	LO5.1
12	**B**	This is a description of adequacy.	LO6.1
13	**C**	See Article 15, UK GDPR	LO7.1
14	**B**	The data protection rights of an individual should not infringe the rights or freedoms of another.	LO7.3
15	**A**	See Article 58, UK GDPR.	LO8.1
16	**C**	See Article 58, UK GDPR.	LO8.1
17	**A**	See Articles 33 & 34, UK GDPR.	LO9.1
18	**D**	Corrections notice does not exist but companies can receive corrective measures.	LO9.2
19	**D**	UK GDPR does not apply to deceased individuals.	LO2.1
20	**D**	Privacy and Electronic Communications Regulations (2003) and UK GDPR always apply to all forms of electronic marketing.	LO10.1