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 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 fulfill a Data Subject Access Request.

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

A Data Minimisation.
B Purpose Limitation.
C Data Encryption.
D Storage Limitation.

4 A company wants to use contact data obtained from business websites and social media profiles to contact companies for marketing purposes.

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

A Consent.
B Business to business.
C Legitimate interests.
D Contract.

5 Which of the following Article 9 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 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 Put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights.
D Ensuring consent is always obtained when processing personal data.

9 Which of the following statements regarding Data Protection Officers 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 To whom does Article 30 - Records of Processing - apply?

A Controllers have sole responsibility for records of processing.
B Processors and controllers are both required to maintain records of processing.
C Processors have sole responsibility for records of processing.
D Processors, controllers and data subjects are each responsible for their own records of processing.

11 When processing personal data under 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 For service messages only.
D Where required to do so by Union or Member State law.

12 What is the purpose of an EU Commission adequacy decision?

A Where adequacy is granted, a company may conduct specific processing of personal data without consent.
B When adequacy is in place, the ICO permits companies to leave databases unencrypted with suitable mitigating controls.
C It's a formal notice that a company may forgo compliance with any one of the data protection principles.
D Companies may execute restricted transfers without further approval where adequacy is in place.

13 You are tasked with creating a company policy for handling Data Subject Requests, select 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 DPO.
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 ICO offer companies in achieving and maintaining compliance with the GDPR?

A Conducting data protection audits for UK companies.
B Advise on appropriate wording for consent statements and privacy policies for your website.

C Provides data protection courses for the public.
D Liaises with the European Data Protection Board (EDPB) on behalf of UK companies.

16 Select the enforcement action that the ICO 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 the 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 A company experiences a theft of a database containing customers personal information.

The ICO investigates and finds the following:

1. The security controls applied to the database were not state of the art.

2. There was no DPIA conducted when the database was implemented, or subsequently.

3. The data subjects were not notified of the breach despite a clear risk to them.

4. This is the first reportable incident the company has experienced.

What is the maximum financial penalty that could be incurred under GDPR?

A 4% of the company's global annual turnover or €20 million.
B £20,000,000.
C €10 million or 2% of the company's global annual turnover.
D £500,000.

19 Your company wishes to contact potential customers to inform them of a change to the products it offers. The current database does not have proper consent under GDPR and there are no suitable grounds for legitimate interests.

What method of communication is **NOT** prohibited by PECR?

A SMS.
B None.
C Letters.
D Business to business (B2B) emails.

20 You've been asked to redesign your companies 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 PECR does not have to meet GDPR specifications.
B PECR applies to B2B marketing, GDPR does not.
C The GDPR replaced the PECR in 2018.
D Electronic marketing campaigns must comply with PECR AND GDPR.

End of Paper

BCS Foundation Certificate in Data Protection
Answer Key

Question	Answer	Syllabus Sections	Rationale
1	**C**	LO1.1.	The GDPR became enforceable on 25 May 2018.
2	**A**	LO2.1.	Pseudonymisation is a technique that replaces or removes information in a data set to render the data subject unidentifiable.
3	**C**	LO2.2.	The GDPR Principles are: Lawfulness, fairness and transparency, Purpose limitation, Data minimisation, Accuracy, Storage limitation, Integrity and confidentiality (security), Accountability.
4	**C**	LO3.1.	Legitimate interest may be used to conduct marketing ONLY in a Business to Business context.
5	**B**	LO3.2.	See GDPR Article 9, 2 (i)
6	**C**	LO4.2.	See Article 35.
7	**B**	LO4.4.	See Article 30.
8	**C**	LO4.6.	Article 25, Data protection by design and default requires that you integrate, or 'bake in' data protection to your systems
9	**C**	LO4.8.	See article 37 – 39, GDPR.
10	**B**	LO5.1.	See article 28 GDPR.
11	**D**	LO5.1.	See article 29, GDPR.
12	**D**	LO6.1.	A country with an adequacy decision is deemed by the EU commission to have suitable data protection measures in place; Article 45, GDPR.
13	**C**	LO7.1.	See Article 15, GDPR
14	**B**	LO7.3.	The data protection rights of an individual should not infringe the rights or freedoms of another.
15	**A**	LO8.1.	See article 58, GDPR.
16	**C**	LO8.1.	See article 58, GDPR.
17	**A**	LO9.1.	See articles 33 & 34, GDPR.

Question	Answer	Syllabus Sections	Rationale
18	**A**	LO9.2.	See Article 83, 5, (a) & (b).
19	**C**	LO10.1.	PECR applies only to electronic communications.
20	**D**	LO10.1.	PECR and GDPR always apply to all forms of electronic marketing.