



BCS Practitioner 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]

Copying of this paper is expressly forbidden without the direct approval of BCS, The Chartered Institute for IT.

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

- 1 Which of the following statements relating to the Human Rights Act is **CORRECT**?
- A The right to respect a private home and family life is an absolute right.
 - B The right to freedom of expression is an absolute right.
 - C The state can infringe on a person's rights in certain prescribed circumstances.
 - D The state cannot infringe on a person's rights and an impact assessment is required to ensure this remains the case.
- 2 With reference to the definitions contained in the GDPR, what statement **BEST** describes the type of data used by fingerprint scanning software?
- A It is genetic data as it recognises the special characteristics of an individual's biology in order to identify a person.
 - B It is biometric data as it processes the physical characteristics of an individual in order to identify a person.
 - C It is biometric data as it processes the behavioural characteristics of an individual in order to identify a person.
 - D It is not genetic data or biometric data as it does not process behavioural characteristics.
- 3 A public authority funds mandatory training sessions for its staff on information security. A database has been set up to record attendance at the scheduled training sessions. As Data Protection Officer, you have been asked to advise on the most appropriate lawful basis for processing.
- Which of the below would be **MOST** suitable under the circumstances?
- A It is likely that they should rely on the lawful basis of consent, and should ask each member of staff for their consent to use their information in the database.
 - B It is likely that they can rely on the lawful basis of public interest task as they are a public authority.
 - C It is likely that they can rely on the lawful basis of legitimate interests as the authority needs to store details of staff who have been trained as a legitimate interest.
 - D It is likely that they can rely on the lawful basis of contract, as employees are bound by contracts of employment.

4 Article 5(2) of the GDPR states:

"The controller shall be responsible for, and be able to demonstrate compliance with [the data protection principles]"

Which of the following does this refer to?

- A The Accountability Principle.
- B Data Protection by Design and Default.
- C Data Protection Impact Assessments.
- D Information Audits.

5 Which of the following is **INCORRECT** in relation to the purpose of a Data Protection Impact Assessment?

- A To consider both the likelihood and the severity of any impact on individuals.
- B To completely eliminate all data protection risks.
- C To mitigate data protection risks.
- D To identify data protection risks.

6 Which of the following items is **NOT** required to be contained within the record of processing activities as set out in the GDPR?

- A Details of staff training.
- B Details of data processing.
- C Details of the Data Subjects.
- D The purpose of processing.

7 Of the following, which does **NOT** illustrate the privacy by design and default approach?

- A Ensuring that Data Protection Impact Assessments consider all of the risks from the start of the project.
- B Ensuring that appropriate technical and organisational measures such as data minimisation or pseudonymisation are put in place.
- C Ensuring that where consent is withdrawn, another lawful basis can be applied if the processing is to continue.
- D Using an agreed certification methods to provide assurances that appropriate safeguards have been put in place to protect personal data.

8 Which of the following is **NOT** an obligation of the processor when processing the Personal Data on behalf of the controller?

- A** Keeping a record of processing activities.
- B** Keeping personal data secure.
- C** Assisting the controller in completing Data Protection Impact Assessments.
- D** Determining the purpose of the processing.

9 From the following list, what information must be included in a Controller - Processor Agreement as specified by Article 28 GDPR?

- a. The subject-matter and duration of the processing
- b. The nature and purpose of the processing
- c. The type of personal data and categories of data subjects
- d. Details of the processor's staff who will have access to the personal data
- e. Obligations and rights of the controller.

- A** a, b, c, and d
- B** a, c, d, and e
- C** a, b, d, and e
- D** a, b, c, and e

10 Select the **CORRECT** response to the following statement:

"Privacy Shield is a framework for regulating exchanges of Personal Data for commercial purposes between the European Union and":

- A** Canada.
- B** The United States of America.
- C** The European Economic Area.
- D** Any country who has received an adequacy decision.

- 11 A government department processes Personal Data in connection with a legal obligation and relies on the Article 6 legal basis of 'Legal Obligation'. Following a recent subject access request, a member of the public notes that their date of birth is incorrect on the record. They write to the department explaining this and insist that they erase all data held about them in accordance with the right to erasure.

What advice is appropriate?

- A They need not do anything. There is a legal obligation to collect the information and they do not need to correct the record.
- B They should erase all records relating to the individual as soon as possible.
- C They should correct the record and inform the individual that the right to erasure doesn't apply.
- D They should inform the individual that they would need to formally complain as individual rights do not apply to this information.

- 12 Of the following statements, which **MOST ACCURATELY** describes the role of the Information Commissioner's Office in relation to data protection legislation?

- A An independent executive non-departmental public body that reports directly to the United Kingdom Parliament as an independent regulatory office.
- B An independent regulatory office, established by the European Commission, and reporting directly to the European Parliament.
- C A public body, led by an Information Commissioner, answerable directly to government ministers to create data protection legislation.
- D A government regulator, answerable only to the Prime Minister of the United Kingdom.

- 13 Which of the following responsibilities does the Information Commissioner's Office **NOT** have?

- A Enforcing the General Data Protection Regulation.
- B Conducting data protection audits.
- C Undertaking Data Protection Impact Assessments for Controllers.
- D Co-operating with other Supervisory Authorities.

- 14 Which of the following is most likely **NOT** to be a personal data breach?
- A The theft of an attendance register from a school.
 - B The loss of a draft public information leaflet on a train.
 - C Sending blood test results to the wrong address.
 - D The accidental destruction of a patient's medical record.
- 15 With reference to the following statement, which of the below endings is **INCORRECT**?
- "In appropriate circumstances, the Information Commissioner may:
- A Instigate criminal proceedings under data protection legislation.
 - B Instigate criminal proceedings under the Computer Misuse Act.
 - C Establish the liability of a Controller and / or Processor.
 - D Order a Controller to compensate a Data Subject.
- 16 Which of the following statements is **INCORRECT** in relation to the lawful basis for processing when offering online services to children?
- A To rely on consent for an information society service, a child must be over the age of 13.
 - B A different lawful basis to consent can be relied on.
 - C The parent or guardian must consent on behalf of any child.
 - D In general, if you are relying on consent as a lawful basis, the child must be competent to give their consent.
- 17 Which of the following statements in relation to the Public Interest Task lawful basis is **INCORRECT**?
- A Can be applied where a task is carried out in the exercise of official authority by a public authority.
 - B Can be applied where a task is carried out in the public interest by a non-public body.
 - C There must be a statutory or common law obligation to undertake the task.
 - D The processing of the information must be necessary.

18 The following statements relate to the differences between GDPR and PECR.

Which statement is **INCORRECT**?

- A** GDPR applies to all marketing using personal data.
- B** PECR relates to marketing by electronic means.
- C** The definition of consent under PECR has been updated by GDPR.
- D** PECR does not apply to business to business communications.

19 What statement **BEST** describes the ICO's Employment Code of Practice?

- A** It must be followed by employers when complying with data protection legislation.
- B** It helps employers in applying employment law in relation to their employees.
- C** It helps employers comply with data protection legislation and encourages them to adopt good practice.
- D** It is designed to help employees understand their rights in relation to data protection legislation.

20 Under the GDPR, which of the following statements is **INCORRECT** in relation to cookies?

- A** A person should be able to withdraw consent to use cookies.
- B** The GDPR applies to the use of any type of cookie.
- C** Implied consent in relation to cookies is insufficient.
- D** Websites must provide an option to opt out of cookies.

End of Paper

BCS Practitioner Certificate in Data Protection Answer Key and Rationale

Question	Answer	Rationale	Syllabus Sections
1	C	The state can restrict a person's right to respect a private home and family life and the right to freedom of expression in prescribed circumstances.	LO1.2.
2	B	Under Article 4(14) GDPR the definition of 'biometric data' specifically includes dactyloscopic data (i.e. fingerprints).	LO2.1.
3	C	It is a legitimate interest of any public authority or other employer to hold information relating to the competence of its employees. It is therefore likely that they can rely on the lawful basis of legitimate interests.	LO3.1.
4	A	This refers to the Accountability Principle as defined in Article 5(2) of the GDPR.	LO4.1.
5	B	The purpose of a data protection impact assessment is to identify, assess and mitigate the risks. While some risks may be mitigated completely, it is not the purpose of the assessment to eliminate all risks.	LO4.2.
6	A	The requirements for the record of processing activity are set out in Article 30. Details of staff training is not a specific requirement.	LO4.4.
7	C	Item C clearly does not illustrate the privacy by design and default approach, whereas the other options do. It would be misleading to a data subject to inform them that consent is the lawful basis being relied on, when they intend to continue to process information relying on another lawful basis should consent be withdrawn.	LO4.6.
8	D	Option D is not an obligation of the Processor, as it would be the controller that would determine the purpose of the processing.	LO5.1.
9	D	A Controller - Processor Agreement does not need to contain details of the processor's staff who will have access to the personal data. All other options are specified by Article 28 of the GDPR.	LO5.4.
10	B	The Privacy Shield is a framework for regulating exchanges of Personal Data for commercial purposes between the European Union and the USA.	LO6.1.
11	C	The right to erasure does not apply to this data. The right to rectification however is likely to apply. The should therefore correct the record and	LO7.1.

Question	Answer	Rationale	Syllabus Sections
		inform the individual that the right to erasure doesn't apply.	
12	A	The ICO is a non-departmental public body that reports directly to the United Kingdom Parliament as an independent regulatory office. The other options have elements which are incorrect.	LO8.1.
13	C	The role of the ICO does not include the undertaking of DPIA's for controllers. This is a responsibility of the Controller.	LO8.2.
14	B	The loss of a draft public information leaflet on a train is not likely to be a personal data breach as it is likely not to contain personal data. All other options clearly contain personal data.	LO9.1.
15	D	A data subject can only claim compensation via the domestic courts. The ICO does not have the power to award compensation.	LO9.5.
16	C	When offering online services to children, a child of 13 and over can consent. It would therefore be incorrect to say that a parent or guardian must consent on behalf of any child. For further explanation please see Article 8 of the GDPR and Section 9 of the DP18. For candidates in Scotland, please refer to Section 208 paragraph 603 of DP18.	LO10.1.
17	C	There need not be a statutory or common law obligation to undertake the task. The overall purpose must be to perform a public interest task or exercise official authority and this must have a sufficiently clear basis in law.	LO11.1.
18	D	PECR does not apply to business to business communications. All other options are correct.	LO12.1.
19	C	The ICO's Employment Code of Practice helps employers comply with data protection legislation and encourages them to adopt good practice.	LO13.1.
20	B	Only cookies which are online cookie identifiers are bound by the GDPR. Where they cannot be used to identify an individual they will not be personal data and therefore GDPR will not apply.	LO13.3.