BCS Practitioner Certificate in Data Protection v9.8

Specimen Paper

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

Specimen paper consists of 20 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: 13/20
Time allowed: 45 minutes

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, which of the following statements **best** describes the type of data used by fingerprint scanning software?

A It is genetic data as the software recognises the special characteristics of an individual's biology in order to identify a person.
B It is biometric data as the software processes the physical characteristics of an individual in order to identify a person.
C It is biometric data as the software processes the behavioural characteristics of an individual in order to identify a person.
D It is not genetic data or biometric data as the software 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 (DPO), you have been asked to advise on the most appropriate lawful basis for processing.

Which of the following would be **most** suitable under the circumstances?

A It is likely that the public authority 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 the public authority can rely on the lawful basis of public interest task as they are a public authority.
C It is likely that the public authority 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 the public authority 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 (DPIA).
D Information audits.

5 When adapting an existing processing activity to utilise AI, which of the following **best** explains why is it important to conduct a Data Protection Impact Assessment (DPIA)?

A To ensure that all employees are aware of their responsibilities when it comes to Artificial Intelligence (AI).
B To assess the risk of Artificial Intelligence (AI) to the organisation's interests.
C To assess whether the use of Artificial Intelligence (AI) is necessary and proportionate to the original purpose and assess against any risks presented by AI.
D To establish clear processes for handling requests to exercise the rights of data subjects.

6 Which of the following items is **not** required to be contained within the Record of Processing Activities (RoPA), 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 Which of the following, does **not** illustrate the privacy by design and default approach?

A Ensuring that Data Protection Impact Assessments (DPIA) 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 (DPIA).
D Determining the purpose of the processing.

9 Which of the following information does **not** have to be included in a controller - processor agreement, as specified by Article 28 GDPR?

A The subject matter and duration of the processing.
B Obligations and rights of the controller.
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.

10 A UK health charity sends personal data to an insurance company, also in the UK. The digital tool that they use to conduct the transfer routes the data through a number of countries outside of the UK, including India. There is no intention that the data will be accessed or manipulated whilst in those countries.

Which of the following statements is **correct** in relation to the above scenario?

A A restricted transfer does not take place, as the data is only in transit.
B A restricted transfer takes place, as the data leaves the UK.
C A restricted transfer takes place, as the data relates to EU citizens.
D A restricted transfer does not take place, as India provides an adequate level of protection for personal data.

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.

Which of the following advice is appropriate for the department to take?

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 does not apply.
D They should inform the individual that they would need to formally complain as individual rights do not apply to this information.

12 Which of the following statements **most** accurately describes the role of the Information Commissioner's Office (ICO) in relation to data protection legislation?

A A 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 (ICO) **not** have?

A Enforcing the GDPR.
B Conducting data protection audits.
C Undertaking Data Protection Impact Assessments (DPIA) for controllers.
D Issuing monetary penalties for data protection breaches.

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 Which of the following endings to the statement below 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 Under UK GDPR, only children aged 13 years and over may lawfully provide their own consent for the processing of their personal data.
B An adult with parental responsibility must provide consent for processing if the child is under 13 and consent is being relied upon.
C There is no requirement under UK GDPR for data controllers to verify that someone providing parental consent has parental responsibility.
D A different lawful basis to consent can be relied upon in certain circumstances.

17 Which of the following statements in relation to the public interest task lawful basis is **incorrect**?

A It can be applied where a task is carried out in the exercise of official authority by a public authority.
B There must be a statutory or common law obligation to undertake the task.
C It can be applied where a task is carried out in the public interest by a non-public body.
D The processing of the information must be necessary.

18 Which of the following statements relating to the differences between UK GDPR and Privacy and Electronic Communications Regulations (PECR) (2003) is **incorrect**?

A UK GDPR applies to all marketing using personal data.
B PECR relates to marketing by electronic means.
C There are different fine regimes for PECR and UK GDPR.
D PECR does not apply to business-to-business communications.

19 Which of the following **best** explains the purpose of the ICO's Employment Practices Guidance?

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

20 Which of the following statements is **incorrect** in relation to cookies under the GDPR?

A A person should be able to withdraw consent to use cookies.
B GDPR only applies to cookies that are not requested or expected by users.
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 v9.8

Answer Key and Rationale

Question	Answer	Rationale	Syllabus Section
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.	1.2
2	**B**	Under Article 4(14) (UK GDPR), the definition of 'biometric data' specifically includes dactyloscopic data (i.e. fingerprints).	2.1
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.	3.1
4	**A**	This refers to the accountability principle, as defined in Article 5(2) of the UK GDPR.	4.1
5	**C**	See the latest ICO guidance on AI and data protection.	14.2
6	**A**	The requirements for the Record of Processing Activity (RoPA) are set out in Article 30 (UK GDPR). Details of staff training is not a specific requirement.	4.4
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.	4.6
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.	5.1
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 UK GDPR.	5.4
10	**A**	See ICO guidance on international transfers and data 'in transit'.	6.1
11	**C**	The right to erasure does not apply to this data. The right to rectification however is likely to apply. They should therefore correct the record and inform the individual that the right to erasure does not apply.	7.1

12	**A**	The Information Commissioner's Office (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.	8.1
13	**C**	The role of the ICO does not include the undertaking of Data Protection Impact Assessments (DPIA) for controllers. This is a responsibility of the controller.	8.2
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.	9.1
15	**D**	A data subject can only claim compensation via the domestic courts. The ICO does not have the power to award compensation.	9.5
16	**C**	UK GDPR requires data controllers to make reasonable efforts to verify that any person giving consent on behalf of a child holds parental responsibility over the child.	10.1
17	**B**	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.	11.1
18	**D**	PECR does apply to business-to-business communications. Read more here: Business-to-business marketing | ICO All other options are correct.	12.1
19	**A**	The guidance is not statutory, so it is not mandatory. It is aimed at organisations and it is about data protection legislation, not employment law.	13.1
20	**B**	Only cookies which are online cookie identifiers are bound by the UK GDPR. Where they cannot be used to identify an individual they will not be personal data and therefore UK GDPR will not apply.	13.3