DUMPSBOSS.

BCS Practitioner Certificate in Data Protection

BCS PDP9

Version Demo

Total Demo Questions: 5

Total Premium Questions: 50

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Context	12
Topic 2, Data Protection Principles	6
Topic 3, Individual Rights	7
Topic 4, Exemptions	4
Topic 5, Enforcement	4
Topic 6, Accountability	13
Topic 7, Privacy and Electronic Communications Regulations (PECR)	4
Total	50

QUESTION NO: 1

How are data sharing practices governed by data protection law?

A. Data sharing practices are covered in the DPA 2018, supported by a statutory Code of Practice that provides specific guidance

B. Data sharing practices are subject to the PECR until the new statutory Code of Practice is published

C. Data sharing practices are covered by the Freedom of Information Act

D. Data sharing practices are not specifically regulated, however the ICO provide best practice guidance

ANSWER: A

Explanation:

Data sharing practices are covered by the Data Protection Act 2018, alongside the UK GDPR's broader requirements for lawful, fair and transparent processing of personal data. The Act gives the Information Commissioner's Office (ICO) the power to prepare a statutory data-sharing code of practice. This is why "Data sharing practices are covered in the DPA 2018, supported by a statutory Code of Practice that provides specific guidance" is correct. The statutory code translates the legal framework into practical expectations for organisations that disclose personal data to another organisation or share it internally. It addresses matters such as identifying a lawful basis, ensuring sharing is necessary and proportionate, being transparent with individuals, applying appropriate security measures, documenting decisions, and using data-sharing agreements where appropriate. Although the code itself does not create an alternative set of data-protection rules, it is an authoritative practical guide to complying with the applicable legislation. The ICO, courts and tribunals may take relevant parts of the code into account when considering whether an organisation has complied with its data-protection obligations. The ICO's Data sharing code of practice provides the guidance, and section 121 of the Data Protection Act 2018 establishes the statutory basis for it.

QUESTION NO: 2

When does a personal data breach need to be reported to a supervisory authority?

A. All personal data breaches must be reported to a supervisory authority

B. Only where a disclosure is of special category data

C. Where the personal data breach is likely to result in a risk to the rights and freedoms of natural persons.

D. When the controller's right of freedom of expression outweighs the data subject's right to a private home and family life.

ANSWER: C

Explanation:

"Where the personal data breach is likely to result in a risk to the rights and freedoms of natural persons." is correct. Under Article 33 of the UK GDPR, a controller must notify the Information Commissioner's Office, as the UK supervisory authority, when it becomes aware of a personal data breach that is likely to result in a risk to individuals' rights and freedoms. Notification must be made without undue delay and, where feasible, within 72 hours of awareness. The assessment is context-specific and should consider both the likelihood and severity of potential consequences for people, including loss of control over personal data, identity fraud, financial loss, discrimination, reputational damage, or loss of confidentiality. The breach notification threshold is "risk"; this is distinct from the higher "high risk" threshold that can require direct communication to affected individuals under Article 34. Controllers remain accountable for recording all personal data breaches, including the facts, effects, and remedial action, even where the risk assessment means notification to the supervisory authority is not required. The ICO's breach guidance confirms that organisations should assess the risk promptly, take steps to contain and remedy the incident, and document the decision. See UK GDPR, Article 33 and the ICO personal data breach guidance.

QUESTION NO: 3

Which of the following statements MOST accurately describes why a risk-based approach to the use of AI is necessary?

A. AI is inherently negative and its use should be limited

B. AI is unlawful

C. AI's benefits make accepting all arising risks necessary.

D. AI carries new and complex risks not present in other technologies

ANSWER: D

Explanation:

AI carries new and complex risks not present in other technologies is correct because artificial intelligence can create or amplify risks to people's rights and freedoms in ways that require careful, context-specific assessment. AI systems may operate at scale, infer information about individuals, make or support consequential decisions, and produce outputs that are difficult for people to understand or challenge. Their use can therefore affect core data-protection principles, including fairness, transparency, accuracy, accountability and security. A risk-based approach means identifying the processing and decision-making impacts that are reasonably likely in the particular use case, assessing their severity and likelihood, and implementing proportionate safeguards before and throughout deployment. Relevant measures may include data-protection impact assessments, meaningful human oversight, testing for bias and accuracy, data minimisation, clear information for affected individuals, and monitoring for changes in performance or impact. This approach enables organisations to realise legitimate benefits from AI while protecting individuals, rather than treating all AI uses identically. The ICO's guidance explains how data-protection law applies to AI and stresses accountability and risk management across the AI lifecycle. See the ICO guidance on AI and data protection and its guidance on data protection impact assessments.

QUESTION NO: 4

Of the following options which is NOT a purpose of carrying out a Data Protection Impact Assessment (DPIA)?

A. It is necessary to fulfil the requirement that all DPIAs are submitted to the ICO

B. It is key to the accountability element of the GDPR.

C. It fulfils a requirement that data protection is carried out by design and default.

D. It assists in identifying the main risks that may exist in any use of data, so that they can be mitigated

ANSWER: A

Explanation:

"It is necessary to fulfil the requirement that all DPIAs are submitted to the ICO" is correct because there is no general GDPR requirement to submit every completed DPIA to the Information Commissioner's Office. A DPIA is an accountability tool used by a controller before commencing processing likely to create a high risk to people's rights and freedoms. It documents the proposed processing, assesses the necessity and proportionality of that processing, identifies privacy risks, and records measures intended to address those risks. The controller must retain the DPIA as part of demonstrating compliance, but routine approval or filing with the ICO is not its purpose.

Contact with the ICO arises only in the specific circumstance of prior consultation. Under Article 36 UK GDPR, a controller must consult the ICO before processing where the DPIA indicates that the processing would result in a high risk in the absence of measures that the controller can take to reduce that risk. Therefore, a DPIA may lead to consultation, but it is not undertaken to satisfy an obligation to submit all DPIAs. This distinction supports a risk-based and proportionate approach to data-protection governance. See the ICO's DPIA guidance and Article 36 GDPR.

QUESTION NO: 5

A payroll provider acting as a processor discovers that a member of its staff sent an employee payroll report to the wrong client. The provider has contained the incident and is assessing its effect.

What is the processor's immediate data protection obligation to its controller client?

A. Notify the controller without undue delay and provide relevant information about the breach

B. Notify the ICO directly within 72 hours because it discovered the breach

C. Notify the affected employees directly because their payroll data was disclosed

D. Wait until the investigation is complete before notifying the controller

ANSWER: A

Explanation:

A processor must notify the controller without undue delay after becoming aware of a personal data breach. The controller is responsible for deciding whether the breach is likely to result in a risk to individuals' rights and freedoms and therefore requires notification to the ICO under Article 33.

The processor should provide the controller with the information reasonably required to assess, contain and document the breach. It should not wait until it has completed every part of its internal investigation, nor should it normally make the regulatory notification itself unless authorised to do so by the controller.