GSDC
Global Skill Development Council

DATA PROTECTION OFFICER: EXAM PREPARATION GUIDE

www.gsdcouncil.org

Questions 1–4

Q1. Under GDPR, a data breach must be reported to the supervisory authority within:

- A) 24 hours of the breach occurring
- B) 72 hours of becoming aware of the breach
- C) 30 days of discovering the breach
- D) 7 days of confirming the breach

✅ **Answer: B**

Q2. Which of the following is NOT a lawful basis for processing personal data under GDPR?

- A) Consent
- B) Legitimate interests
- C) Commercial benefit
- D) Legal obligation

✅ **Answer: C**

Q3. A DPO MUST be appointed when an organization:

- A) Has more than 50 employees
- B) Processes any personal data online
- C) Carries out large-scale systematic monitoring of individuals as a core activity
- D) Uses cookies on their website

✅ **Answer: C**

Q4. Under GDPR, the right to data portability applies when processing is based on:

- A) Legitimate interests or legal obligation
- B) Consent or contract — and processing is automated
- C) Vital interests or public task
- D) Any lawful basis

✅ **Answer: B**

Questions 5–8

Q5. Which GDPR principle requires that personal data is not kept longer than necessary?

- A) Data minimisation
- B) Purpose limitation
- C) Storage limitation
- D) Accuracy

✅ **Answer: C**

Q6. The upper tier of GDPR administrative fines can reach:

- A) €10 million or 2% of global annual turnover
- B) €20 million or 4% of global annual turnover
- C) €50 million or 5% of global annual turnover
- D) €5 million or 1% of global annual turnover

✅ **Answer: B**

Q7. Which statement about a DPO is TRUE?

- A) The DPO is personally liable for all data protection breaches
- B) The DPO must always be an internal employee
- C) The DPO must report directly to the highest level of management
- D) The DPO approves all data processing decisions

✅ **Answer: C**

Q8. Which transfer mechanism is most commonly used for international data transfers where no adequacy decision exists?

- A) Binding Corporate Rules
- B) Derogations
- C) Standard Contractual Clauses
- D) Certification schemes

✅ **Answer: C**

Questions 9–12

Q9. A DPIA is mandatory BEFORE processing begins when:

- A) Any new IT system is launched
- B) Processing is likely to result in high risk to individuals
- C) More than 100 individuals' data will be processed
- D) A new member of staff joins the data protection team

✅ **Answer: B**

Q10. An individual requests erasure of their personal data. The organization CAN refuse if the data is required for:

- A) Internal analytics and reporting
- B) Direct marketing purposes
- C) The exercise or defense of legal claims
- D) Improving customer experience

✅ **Answer: C**

Q11. Which of the following is considered sensitive / special category data under GDPR?

- A) Email address
- B) Job title
- C) Biometric data used for identification
- D) Home address

✅ **Answer: C**

Q12. What is the standard response timeframe for a Subject Access Request under GDPR?

- A) 15 days
- B) 30 days
- C) 45 days
- D) 60 days

✅ **Answer: B**

Questions 13–16

Q13. Under GDPR, pseudonymised data is:

- A) No longer considered personal data
- B) Still considered personal data
- C) Treated the same as anonymised data
- D) Exempt from all GDPR obligations

✅ **Answer: B**

Q14. Which of the following best describes the role of a Data Processor?

- A) Determines the purpose and means of processing personal data
- B) Processes personal data on behalf of and under instructions from the controller
- C) Approves all data protection policies within the organization
- D) Decides which lawful basis applies to each processing activity

✅ **Answer: B**

Q15. Under GDPR, consent must be:

- A) Implied from the individual's behavior
- B) Freely given, specific, informed, and unambiguous
- C) Obtained once and valid indefinitely
- D) Confirmed by a signed paper form only

✅ **Answer: B**

Q16. How many data protection principles are outlined in GDPR?

- A) 5
- B) 6
- C) 7
- D) 8

✅ **Answer: C**

Questions 17–20

Q17. Which GDPR principle requires the controller to be able to demonstrate compliance?

- A) Integrity and confidentiality
- B) Purpose limitation
- C) Accountability
- D) Lawfulness

✅ **Answer: C**

Q18. Under GDPR, when can a controller charge a fee for a Subject Access Request?

- A) For every request submitted
- B) When the request involves more than 50 records
- C) Only when the request is manifestly unfounded or excessive
- D) When the requester has made more than one request per year

✅ **Answer: C**

Q19. Which of the following is an example of a technical security measure under GDPR?

- A) Staff confidentiality agreements
- B) Encryption of personal data at rest and in transit
- C) A data protection training program
- D) An organizational privacy policy

✅ **Answer: B**

Q20. The right to object to direct marketing under GDPR is:

- A) Subject to a balancing test by the controller
- B) Only available to customers — not employees
- C) Absolute — the controller must always comply
- D) Only available if the individual can provide a reason

✅ **Answer: C**

Questions 21–24

Q21. Under GDPR, which organization has authority to investigate complaints and impose fines?

- A) The Data Controller
- B) The European Court of Justice
- C) The Supervisory Authority
- D) The Data Processor

✅ **Answer: C**

Q22. A Binding Corporate Rule (BCR) is used for:

- A) Transfers between unrelated companies in different countries
- B) International data transfers within a multinational corporate group
- C) Processing employee data across multiple departments
- D) Transfers to countries with an adequacy decision

✅ **Answer: B**

Q23. Under GDPR, what is the default minimum age for a child to provide valid consent for online services?

- A) 13 years
- B) 14 years
- C) 16 years
- D) 18 years

✅ **Answer: C**

Q24. Which of the following processing activities is MOST likely to require a DPIA?

- A) Maintaining an employee telephone directory
- B) Sending a monthly newsletter to opted-in subscribers
- C) Large-scale processing of health data using AI profiling
- D) Storing customer invoices for 7 years

✅ **Answer: C**

Questions 25–28

Q25. Under GDPR, the legitimate interests lawful basis requires which three-part assessment?

- A) Consent, contract, and compliance
- B) Purpose, necessity, and balancing
- C) Risk, impact, and mitigation
- D) Scope, duration, and review

✅ **Answer: B**

Q26. A Data Processing Agreement (DPA) between a controller and processor must require the processor to:

- A) Determine the purposes of processing independently
- B) Process data only on documented instructions from the controller
- C) Appoint its own DPO regardless of size
- D) Retain all personal data indefinitely for audit purposes

✅ **Answer: B**

Q27. Which of the following is TRUE about the right to erasure under GDPR?

- A) It is an absolute right with no exceptions
- B) It applies only to data collected via consent
- C) It can be refused when data is needed for legal claims
- D) It must be fulfilled within 72 hours

✅ **Answer: C**

Q28. Which privacy framework primarily governs data protection in Brazil?

- A) PDPA
- B) PIPEDA
- C) POPIA
- D) LGPD

✅ **Answer: D**

Questions 29–32

Q29. Under GDPR, which of the following is NOT required in a breach notification to a supervisory authority?

- A) The name and address of every affected individual
- B) Categories of personal data affected
- C) Approximate number of individuals affected
- D) Measures taken or proposed to address the breach

✅ **Answer: A**

Q30. Privacy by Design requires that privacy is:

- A) Added to a system after it is built and tested
- B) Considered only for high-risk processing activities
- C) Embedded into the design and architecture of systems from the start
- D) Applied only when sensitive data is involved

✅ **Answer: C**

Q31. Under GDPR, if a controller cannot meet the 1-month response deadline for a Subject Access Request, they may extend it by:

- A) 1 additional month
- B) 2 additional months
- C) 3 additional months
- D) 6 additional months

✅ **Answer: B**

Q32. Which of the following describes an adequacy decision?

- A) A court ruling confirming that a data breach was not serious
- B) A European Commission decision that a third country provides adequate data protection
- C) An internal assessment confirming a DPA meets GDPR standards
- D) A certification confirming an organization's GDPR compliance

✅ **Answer: B**

Questions 33–36

Q33. Which GDPR principle requires that personal data is collected only for specified, explicit, and legitimate purposes?

- A) Data minimisation
- B) Accuracy
- C) Purpose limitation
- D) Storage limitation

✅ **Answer: C**

Q34. Under GDPR, which of the following is an example of an organizational security measure?

- A) Encrypting a database
- B) Installing a firewall
- C) Conducting regular staff data protection training
- D) Enabling multi-factor authentication

✅ **Answer: C**

Q35. A ROPA (Record of Processing Activities) is mandatory for organizations with 250 or more employees. It is ALSO required for smaller organizations when they:

- A) Have a website that uses cookies
- B) Employ a DPO
- C) Regularly process special category data
- D) Operate in more than one country

✅ **Answer: C**

Q36. Under GDPR, which right allows an individual to receive their personal data in a structured, commonly used, and machine-readable format?

- A) Right to access
- B) Right to rectification
- C) Right to erasure
- D) Right to data portability

✅ **Answer: D**

Questions 37–40

Q37. A data processor discovers a security incident affecting personal data. Under GDPR, the processor must notify the controller:

- A) Within 72 hours of becoming aware
- B) Within 24 hours of becoming aware
- C) Without undue delay
- D) Within 30 days of becoming aware

✅ **Answer: C**

Q38. Which of the following best describes anonymised data under GDPR?

- A) Data that has been encrypted and can be decrypted by the controller
- B) Data that has been irreversibly altered so individuals can no longer be identified
- C) Data stored under a pseudonym that can be reversed using a key
- D) Data that has had the individual's name removed

✅ **Answer: B**

Q39. Under GDPR, the lower tier of administrative fines applies to violations of:

- A) Core principles, individual rights, and international transfers
- B) Technical and organizational obligations such as data processor obligations
- C) Obligations related to children's data only
- D) Breach notification obligations only

✅ **Answer: B**

Q40. Which of the following is a key requirement for valid consent under GDPR?

- A) Consent can be bundled with terms and conditions
- B) Silence or inactivity constitutes valid consent
- C) Pre-ticked boxes can be used where the purpose is clear
- D) Individuals must be able to withdraw consent as easily as they gave it

✅ **Answer: D**

GSDC
Global Skill Development Council

DATA PROTECTION OFFICER CERTIFICATION

ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING OBJECTIVE

- Gain insights into autonomous decision-making processes
- Apply knowledge using ready-to-implement templates
- Demonstrate ability to work with Agentic AI models
- Validate your skills wit

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org