◇ EASY (Q1–Q10)

Q1. GDPR primarily aims to protect:
A. Corporate intellectual property
B. Personal data and privacy of individuals
C. Network infrastructure
D. Financial transactions

Q2. GDPR came into effect on:
A. 1 January 2016
B. 25 May 2018
C. 1 April 2020
D. 1 July 2019

Q3. Which entity determines the purpose and means of processing personal data?
A. Data Processor
B. Data Subject
C. Data Controller
D. Supervisory Authority

Q4. GDPR applies to organizations that:
A. Are based only in the EU
B. Process data of EU residents
C. Use cloud services
D. Store financial data

Q5. Which of the following is considered personal data under GDPR?
A. Encrypted system logs only
B. Anonymized statistics
C. IP address linked to a user
D. Public company revenue

Q6. Which GDPR principle requires data to be collected for specified purposes only?
A. Accuracy
B. Data minimization
C. Purpose limitation
D. Accountability

Q7. Sensitive personal data under GDPR is referred to as:
A. Confidential data
B. Restricted data
C. Special category data
D. Classified data

Q8. Which right allows individuals to obtain a copy of their personal data?
A. Right to erasure
B. Right of access
C. Right to object
D. Right to restriction

Q9. GDPR emphasizes which core governance concept?
A. Automation
B. Accountability
C. Outsourcing
D. Certification

Q10. GDPR is best described as a:
A. Technical standard
B. Voluntary framework
C. Regulation
D. Industry guideline

◇ MEDIUM (Q11–Q25)

Q11. Which of the following is NOT a GDPR principle?
A. Lawfulness, fairness, transparency
B. Storage limitation
C. Confidentiality by default
D. Integrity and confidentiality

Q12. Which data category requires additional protection under GDPR?
A. Employee ID
B. Health records
C. Email address
D. Username

Q13. Lawful processing under GDPR requires at least one:
A. Security control
B. Lawful basis
C. Encryption mechanism
D. Audit report

Q14. The “right to be forgotten” refers to:
A. Data encryption
B. Data minimization
C. Right to erasure
D. Right to restrict processing

Q15. Which role must be appointed in certain GDPR-regulated organizations?
A. Chief Information Officer
B. Data Protection Officer
C. Compliance Manager
D. Security Auditor

Q16. Data Protection Impact Assessments (DPIA) are required when:
A. Processing is low risk
B. Processing involves high risk to individuals
C. Data is anonymized
D. Processing is outsourced

Q17. GDPR breach notification generally requires reporting within:
A. 24 hours
B. 48 hours
C. 72 hours
D. 7 days

Q18. Which principle requires organizations to be able to demonstrate compliance?
A. Transparency
B. Integrity
C. Accountability
D. Purpose limitation

Q19. Which of the following is a responsibility of data processors?
A. Determining processing purpose
B. Ensuring lawful basis
C. Processing data on controller instructions
D. Defining retention period

Q20. GDPR penalties are primarily based on:
A. Fixed monetary fines
B. Percentage of global turnover
C. Number of data subjects
D. Length of data breach

Q21. Which right allows individuals to move their data between service providers?
A. Right to access
B. Right to portability
C. Right to rectification
D. Right to object

Q22. Which GDPR concept limits data collection to what is necessary?
A. Purpose limitation
B. Data minimization
C. Storage limitation
D. Accuracy

Q23. Which entity enforces GDPR compliance?
A. ISO
B. PCI SSC
C. Supervisory Authorities
D. World Economic Forum

Q24. GDPR treats pseudonymized data as:
A. Anonymous data
B. Non-personal data
C. Personal data
D. Public data

Q25. Which GDPR obligation MOST directly supports privacy by design?
A. Incident response
B. Encryption
C. Integrating privacy into processing activities
D. Annual audits

△ HARD (Q26–Q40)

Q26. Which scenario BEST illustrates extraterritorial applicability of GDPR?
A. EU company processing EU data
B. Non-EU company offering services to EU residents
C. EU company processing employee payroll
D. Government data processing

Q27. An organization relying solely on consent for processing faces risk because:
A. Consent is always valid
B. Consent can be withdrawn
C. Consent is mandatory
D. Consent eliminates accountability

Q28. Which GDPR principle MOST directly addresses excessive data retention?
A. Accuracy
B. Data minimization
C. Storage limitation
D. Purpose limitation

Q29. Which condition permits processing of special category data?
A. Business convenience
B. Explicit consent or legal obligation
C. Data encryption
D. Anonymization

Q30. Which GDPR penalty tier is applied for violations of core principles?
A. Lower tier only
B. Administrative warning
C. Higher tier (up to 4% turnover)
D. No penalty

Q31. Which governance failure MOST increases GDPR non-compliance risk?
A. Regular audits
B. Lack of data inventory
C. Encryption
D. Incident response plan

Q32. GDPR accountability requires organizations to:
A. Prevent all breaches
B. Prove compliance proactively
C. Encrypt all data
D. Appoint external auditors

Q33. Which right MOST impacts automated decision-making systems?
A. Right to access
B. Right to rectification
C. Rights related to profiling
D. Right to portability

Q34. A GDPR-compliant organization without security controls would MOST likely:
A. Remain compliant
B. Face integrity and confidentiality violations
C. Eliminate risk
D. Avoid penalties

Q35. Which GDPR requirement MOST closely aligns with cybersecurity governance?
A. Cookie consent
B. Privacy by design and default
C. Data subject consent forms
D. Marketing preferences

Q36. Which factor MOST complicates GDPR compliance for global organizations?
A. Single jurisdiction
B. Cross-border data transfers
C. Local data storage
D. Limited users

Q37. Which GDPR principle links legal compliance with ethical responsibility?
A. Accountability
B. Transparency
C. Lawfulness, fairness, transparency
D. Integrity

Q38. An organization that documents policies but ignores enforcement violates which principle MOST?
A. Accuracy
B. Accountability
C. Storage limitation
D. Data minimization

Q39. GDPR MOST strongly shifts responsibility towards:
A. Data subjects
B. Regulators
C. Organizations processing data
D. Technology vendors

Q40. The PRIMARY objective of GDPR is to:
A. Enable free data flow without controls
B. Protect individual privacy rights
C. Promote encryption standards
D. Replace cybersecurity frameworks