### Exam for the GDPR Practitioner

(Multiple Choice)

**Ques 1. \_\_\_\_\_\_ is an international treaty to protect human rights and fundamental freedoms in Europe.**

1. The General Data Protection Regulation (GDPR)
2. The European Convention on Human Rights (ECHR)
3. The member states of the European Union
4. The European Court of Human Rights

Answer: b) the European Convention on Human Rights (ECHR)

Explanation: The European Convention on Human Rights (ECHR) (formally the Convention for the Protection of Human Rights and Fundamental Freedoms) is an international treaty to protect human rights and fundamental freedoms in Europe.

**Ques 2. Which of the following is not included in the preparatory steps of the GDPR?**

1. Coping with the Brexit
2. Risk Analysis
3. Gap Analysis
4. Quality Analysis & Improving

Answer: d)

Explanation: Steps to prepare your organization for the GDPR includes - Gap analysis, Risk analysis, Project steering and resource/budget planning, Implementation of a data protection structure, Local Add-on Requirements and Coping with the Brexit.

**Ques 3. Under the GDPR compliances, when you collect personal data you need to provide data subject certain information. Which of the following is not included in that information?**

1. Lawful basis for processing the data
2. Organization Internal information
3. Data Retention Period
4. Individual Rights or data subject rights

Answer: b) Organization Internal Information

Example: An organization will need to explain their lawful basis for processing the data; data subject’s data retention periods and that individual have a right to complain to the ICO if they think there is a problem with the way organization handling their data.

**Ques 4. Will Brexit make the GDPR compliance invalid?**

1. Yes
2. No
3. Not sure
4. I don’t know

Answer: b) No

Explanation: The answer is No. The UK is set to go full Brexit on 29th March 2019 and the GDPR comes into effect for EU nations from 25th May 2018, that means there’s at least a year of GDPR compliance to prepare for, whether UK leave the EU or somehow brush Article 50 under the rug, whistling inconspicuously, and pretending this never happened.

**Ques 5. According to GDPR, a set of rules and principles that ensure an adequate level of protection of international transfers of personal data within the same corporate group is termed as:**

1. Consent
2. Binding Corporate Rules (BCRs)
3. Documentation
4. Encryption policies

Answer: b) Binding Corporate Rules (BCRs)

Explanation: According to GDPR, Binding Corporate Rules (BCR) are a set of rules and principles that ensure an adequate level of protection of international transfers of personal data within the same corporate group.

**Ques 6. Implement measures that meet the principles of data protection by design and data protection by default doesn’t include:**

1. Data Minimization
2. Transparency
3. Allowing individuals to monitor processing
4. Standard contractual clauses

Answer: d) Standard contractual clauses

Explanation: Implement measures that meet the principles of data protection by design and data protection by default. Measures could include data minimization, Pseudonymisation, transparency, allowing individuals to monitor processing and creating and improving security features on an ongoing basis.

**Ques 7. Is “the requirement for organizations to register (‘notify’) national Data Protection Authorities (DPAs) of the intended processing activities” is considered under the Accountability Principle of the GDPR?**

1. Yes
2. No
3. Not Sure
4. I don’t know

Answer: a) Yes

Explanation: The concept of ‘Accountability’, imposes on organization various obligation one of them is the requirement for organizations to register (‘notify’) national Data Protection Authorities (DPAs) of the intended processing activities.

**Ques 8. Why is GDPR a concern for Non-EU countries?**

1. Because they are dealing with data of EU citizens
2. Non-EU organizations need not to concern as they are not from another country
3. GDPR applies to every company who has even one customer in Europe regardless of its geographical location
4. Both (a) and (c)
5. Only (a)

Answer: d) Both (a) and (c)

Explanation: GDPR applies to every company who has even one customer in Europe and therefore has far-reaching consequences for multi-nationals and e-commerce businesses that trade across borders.

**Ques 9. The maximum fine that can be imposed for the most serious infringements, such as not having sufficient customer consent to process data, is**

1. 4% of annual turnover
2. 20 million Euros
3. 2% of global annual turnover
4. Both (a) and (b)
5. All (a), (b) and (c)

Answer: e), all (a), (b) and (c) according to the extent of the violation of the regulation

Explanation: The maximum fine that can be imposed for the most serious infringements, such as not having sufficient customer consent to process data, is 4% of annual global turnover or €20 million (whichever is greater). For less serious infringements, such as failure to notify about a breach, a fine of up to 2% of global annual turnover would apply.

**Ques 10. Consider the example and choose the correct option: “if you have inaccurate personal data and have shared this with another organization, you will have to tell the other organization about the inaccuracy so it can correct its own records.” You won’t be able to do this unless you know:**

1. Compliance problems under the GDPR
2. The way you are handling data of data subjects
3. What personal data your organization holds
4. Effective policies and procedures

Answer: c) What personal data your organization holds

Explanation: The GDPR requires you to maintain records of your processing activities. You should document what personal data you hold, where it came from, and who you share it with. You may need to organize an information audit across the organization or within particular business areas.

**Ques 11. “If your organization handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly.” This statement is defined under which of the following:**

1. Subject Access Request
2. Individual’s Rights
3. Consent
4. Communication Privacy Information

Answer: a) Subject Access Request

Explanation: Under Subject Access Request, if your organization handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly then you are required to update your procedures and plans for handling requests to take account of new rules under GDPR.

**Ques 12. As mentioned under Article 5(2) of the GDPR, the accountability principle requires you to:**

1. Review your contracts with vendors
2. Assign ownership and budget for data protection compliance
3. To demonstrate that you comply with the principles and states explicitly that this is your responsibility
4. To have clear documentation and recording procedures

Answer: c) To demonstrate that you comply with the principles and states explicitly that this is your responsibility

Explanation: The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

**Ques 13. Under which Article of GDPR organizations are allowed to transfer data (under defined conditions) to a third country or an international organization.**

1. Article 47
2. Article 46
3. Article 49
4. Article 45

Answer: c) Article 49

Explanation: Under Article 49 of the GDPR that is Derogations for specific situations, in the absence of an adequacy decision pursuant or of appropriate safeguards pursuant, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only on some defined conditions.

**Ques 14. Under which article the GDPR gives data subjects the right to withdraw consent at any time.**

1. Article 8
2. Article 9
3. Article 7
4. Article 6

Answer: c) Article 7

Explanation: Under Article 7(3) of the GDPR gives data subjects the right to withdraw consent at any time and “it shall be as easy to withdraw consent as to give it.” Controllers must inform data subjects of the right to withdraw before consent is given.

**Ques 15. Is the famous “Snowden's global surveillance disclosures” is accused of violating the Article 8 of the European Convention on Human Rights?**

1. No
2. Yes
3. Only allow for the targeted surveillance related to serious crime or terrorism
4. Not Sure

Answer: b) Yes

Explanation: The top official for counter-terrorism and human rights condemned that the mass electronic surveillance as a clear violation of core privacy rights guaranteed by multiple treaties and conventions and makes a distinction between targeted surveillance. Only targeted interception of traffic and location data in order to combat serious crime, including terrorism, is justified, according to a decision by the European Court of Justice.

**Ques 16. Consider an example, “password sharing puts any enterprise at risk of data loss as the password security system is a vulnerable protocol” what do you think is this example considered as a violation of the GDPR compliance?**

1. Yes
2. No
3. I don’t know
4. I’m not sure

Answer: a) Yes

Explanation: GDPR regulation mandates monitoring for data leakage from negligent or malicious employees and external data theft is a salient component that’s why the above-mentioned example is considered to violates the GDPR compliances.

**Ques 17. You must designate a DPO if you are**

1. An organization that carries out the regular and systematic monitoring of individuals on a large scale
2. A public authority (except for courts acting in their judicial capacity)
3. Both (a) and (b)
4. Only (a)

Answer: c) Both (a) and (b)

Explanation: You must designate a DPO if you are a public authority (except for courts acting in their judicial capacity), an organization that carries out the regular and systematic monitoring of individuals on a large scale, an organization that carries out the large-scale processing of special categories of data, such as health records, or information about criminal convictions.

**Ques 18. Along with the implementation of appropriate technical and organizational measures against unauthorized or unlawful processing of data, it also requires implementation of appropriate technical and organizational against which of the following:**

1. Accidental loss of data
2. Encrypted Data
3. Sensitive Data
4. None of these

Answer: a) Accidental loss of data

Explanation: Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. This is the seventh data protection principle.

**Ques 19. On the basis of the Accountability principle, Gap Analysis requires you to identify**

1. Any shortfalls and an implementation plan to address such gaps
2. All internal and external parties involved in your processing
3. Review of internal and public-facing policies and procedures
4. None of these

Answer: a) any shortfalls and an implementation plan to address such gaps

Explanation: A gap analysis based on the Accountability requirements to identify any shortfalls and an implementation plan to address such gaps.

**Ques 20. There are four express protected interests under Article 8. Under which of the following circumstances public authorities can interfere these protected interests.**

1. For general awareness
2. For Government work
3. For Collecting data
4. For public safety or the economic well-being of the country

Answer: d) For public safety or the economic well-being of the country

Explanation: There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

**Ques 21. Which Article states that the controllers will not have to erase or rectify data after the data subject has withdrawn consent?**

1. Article 89
2. Article 70
3. Article 45
4. Article 43

Answer: a) Article 89

Explanation: Under Article 89, it is mentioned that the controllers will not have to erase or rectify data after the data subject has withdrawn consent.

**Ques 22. If personal data is transferred from Europe to a country outside the European Union/European Economic Area then:**

1. Additional employment-related requirements may exist regarding the processing of HR data
2. Organization that transfer data to organization outside the EU will no longer be part of the European Union in near future
3. Transferred data may result in a high risk to the rights and freedoms of natural persons
4. Data processing agreements must be concluded

Answer: d) Data processing agreements must be concluded

Explanation: Due to the high number of agreements to be concluded with internal and external parties, a sensible data processing contract management strategy will have to be implemented. If personal data is transferred from Europe to a country outside the European Union/European Economic Area, data processing agreements must often also be concluded.

**Ques 23. The BCR does not provide a basis for transfers**

1. Made within the EU states
2. Made outside the EU group
3. Made among the EU cooperation
4. All of these

Answer: b) Made outside the EU group

Explanation: Once approved under the EU cooperation procedure, BCR provides a sufficient level of protection to companies to get authorization of transfers by national data protection authorities ("DPA"). The BCR does not provide a basis for transfers made outside the group.

**Ques 24. How will GDPR change the way company’s approaches data Privacy?**

1. Because of Data Subject Right
2. Provision of Penalties
3. Requirement of Consent
4. All of these

Answer: d) All of these

Explanation: The key points of the GDPR that will change the way the company approaches data privacy defines increased territorial scope, provision of penalties, consent, and most importantly, data subject’s rights.

**Ques 25. Which of the following special data processing is not mentioned under the Explicit consent**?

1. The processing of genetic data
2. The Processing of general data like name, address, etc.,
3. The processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs
4. The Processing of data concerning a natural person's sex life or sexual orientation

Answer: b) The Processing of general data like name, address, etc.

Explanation: GDPR Article 9 defines a higher level of consent explicit consent for the processing of special categories of personal data. These special categories include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, the processing of genetic data, biometric data for the purpose uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**Ques 26. If your organization offers online services to children and relies on consent to collect information about them, the GDPR sets the age when a child can give their own consent. What is the age sets by GDPR?**

1. 16 years
2. 16 years and lowered to 13 in the UK
3. 13 years
4. 15 years

Answer: b) 16 years and lowered to 13 in the UK

Explanation: For the first time, the GDPR will bring in special protection for children’s personal data, particularly in the context of internet services such as social networking. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding ‘parental responsibility’.

**Ques 27. The accountability measures mandated under the GDPR does not include**

1. Data Subjects
2. Internal Records
3. Privacy Impact Assessments
4. Member State lawsuits

Answer: d) Member State lawsuits

Explanation: The accountability measures mandated under the GDPR includes Data Subjects, Internal Records, Private Impact Assessment, Suppliers, and Data Processing Officers.

**Ques 28. Once consent is withdrawn, is there any Right of data subjects which they can exercise or use?**

1. They have right to have their personal data erased
2. They can claim that organization no longer used data subject’s personal data for processing
3. Once consent is withdrawn no right is given to data subjects
4. Both (a) and (c)
5. Both (a) and (b)

Answer: e) Both (a) and (b)

Explanation: Article 7(3) states that once consent is withdrawn, data subjects have the right to have their personal data erased and no longer used for processing.

**Ques 29. If your organization operates in more than one EU member state then you should determine your \_\_\_\_\_\_\_\_ and document this.**

1. Data Controller
2. Data Processor
3. Legal Advisory
4. Lead data protection supervisory authority

Answer: d) Lead data protection supervisory authority

Explanation: If your organization operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this. The lead authority is the supervisory authority in the state where your main establishment is.

**Ques 30. In regard of the example, “in compliance with the principles set out by with article 25 and 26 of the European Directive 95/46 for all flows of data within the group which are covered by the scope of the BCR”, what do you think, is this example is consider as an advantage of implementing BCRs?**

1. No
2. Yes
3. Not sure
4. I Don’t know

Answer: b) Yes

Explanation: BCR makes it possible to be in compliance with the principles set out in articles 25 and 26 of the European Directive 95/46 for all flows of data within the group which is covered by the scope of the BCR, which is one of the most important examples of the BCRs.

**Ques 31. Continuous Monitoring is provided as a solution to which of the following:**

1. To develop a more continuous view into the state of compliance of the processing of personal data with the GDPR
2. To mandates monitoring for data leakage from negligent or malicious employees and external data theft
3. To handling data of data subjects
4. To Project steering and resource/budget planning

Answer: a) to develop a more continuous view into the state of compliance of the processing of personal data with the GDPR

Explanation: The answer to the problem of superficial compliance is to develop a more continuous view into the state of compliance of the processing of personal data with the GDPR and in particular to mitigate the risk involved for the data subject through the establishment of near real-time risk management with strong and effective continuous monitoring and response processes.

**Ques 32. 'Informed consent' is a lawful basis to process personal data under the General Data Protection Act (GDPR). The purpose of the processing for which consent is given should be documented. At what time in the process should the data subject's consent be obtained?**

1. After the purpose specification is presented and before personal data is collected.
2. Before the purpose specification is conceived and presented.
3. Before the personal data is processed.
4. Before the personal data is published or disseminated

Answer: a) After the purpose specification is presented and before personal data is collected.

Explanation: Consent can only be informed after the purpose specification is presented to the data subject.

**Ques 33. It has been ascertained that a data breach of sensitive personal data occurred. To whom must this ultimately be reported according to the General Data Protection Regulation (GDPR)?**

1. the Data Protection Authority (DPA)
2. the Data Protection Officer (DPO)
3. the manager of the department
4. the police

Answer: a) the Data Protection Authority (DPA)

Explanation: Data breaches must be reported to the DPA if they might have a significant impact on the security of the data subject or their personal data.

**Ques 34. Together with continuous monitoring of the specific compliance arrangements, continuous improvement and near real-time reporting, which of the following is also necessary:**

1. Data Processing Agreements
2. Regular and systematic monitoring of individuals
3. Subject Access Request
4. Effective processes with measurement-based outcomes

Answer: d) Effective processes with measurement-based outcomes

Explanation: Effective processes with measurement-based outcomes are necessary, together with continuous monitoring of the specific compliance arrangements, continuous improvement and near real-time reporting.

**Ques 35. One of the objectives of a Privacy Impact Assessment (PIA) is to ‘strengthen the confidence of customers or citizens in the way personal data is processed and privacy is respected’. How can a PIA 'strengthen the confidence'?**

1. The organization minimizes the risk of costly adjustments in processes or redesign of systems in a later stage.
2. The organization prevents non-compliance to the GDPR and minimizes the risk of fines.
3. The organization proves that it takes privacy seriously and aims for compliance to the GDPR.

Answer: c) The organization proves that it takes privacy seriously and aims for compliance to the GDPR.

Explanation: In order to 'strengthen the confidence' the organization proves that it takes privacy seriously and aims for compliance to the GDPR.

**Ques 36. Which of the following is not the benefit of the Continuous monitoring?**

1. Identifying and categorizing personal data
2. Authorizing the processing of personal data
3. Standard contractual clauses
4. Implement technical and organizational measures

Answer: c) Standard contractual clauses

Explanation: The benefit of continuous monitoring include Identification and categorization of personal data, authorization of the processing of the personal data and implementation of technical and organizational measures.

**Ques 37. Which of the following is considered as the sample measure for monitoring performance?**

1. Ownership and budget for data protection compliance
2. Percentage of processing of personal data not adapted to the principles and rules of the GDPR
3. Internal and external parties involved in your processing
4. Get authorization of transfers by national data protection authorities

Answer: b) Percentage of processing of personal data not adapted to the principles and rules of the GDPR.

Explanation: The sample measure for monitoring performance include Percentage of processing of personal data not adapted to the principles and rules of the GDPR, Number of exceptions to privacy management architecture standard, Percentage of architectural domains that comply with GDPR obligations, etc.

**Ques 38. Requirements analysis must begin with understanding the \_\_\_\_\_\_\_\_ and stating clearly which aspects the continuous monitoring program is intended to address. Fill in the blank with the correct option.**

1. EU laws
2. Data Minimization and Encryption policies
3. Process monitoring
4. GDPR obligations

Answer: d) GDPR obligations

Explanation: Requirements analysis must begin with understanding the GDPR obligations and stating clearly which aspects the continuous monitoring program is intended to address. This requires a true understanding of the organization’s business and operational processes and goals, as well as barriers to achieving these goals.

**Ques 39. Which of the following is the most important of all activities to ensure that the requirements analysis is done properly?**

1. System Development Lifecycle
2. Cybersecurity controls
3. Privacy management architecture standard
4. Timeliness and completeness of data subject risk profiles

Answer: a) System Development Lifecycle

Explanation: With every system development lifecycle, ensuring that the requirements analysis is done properly is the most important of all activities. If requirements are not valid and complete, all activity that follows will go in the wrong direction.

**Ques 40. Demonstrating an appropriate level of security generally appears difficult without which of the following measures.**

1. Security of internal networks
2. Logical access control
3. Security and authorization policy
4. All of these

Answer: d) All of these

Explanation: Demonstrating an appropriate level of security generally appears difficult without the following measures: Security and authorization policy, Logical access control, Patch management Secured Internet connection, Security of internal networks, etc.

**Ques 41. The EU General Data Protection Regulation (GDPR) is unique in the field of compliance standards for its establishment of financial penalties for:**

1. Allowing Individual to monitor processing
2. Communicating privacy information
3. the loss or mismanagement of personal data of EU citizens
4. transferring data outside the EU

Answer: c) the loss or mismanagement of personal data of EU citizens

Explanation: The EU General Data Protection Regulation (GDPR) is unique in the field of compliance standards for its establishment of financial penalties for the loss or mismanagement of personal data of EU citizens. And, those fines are higher and more likely to be assessed than any existing standard.

**Ques 42. Which of the following is considered as the key pillar of the EU GDPR and also a key means of documenting that your security is up to snuff?**

1. Data Encryption
2. Vulnerability Assessment
3. Data Minimization
4. Data Redundancy

Answer: b) Vulnerability Assessment

Explanation: Vulnerability Assessment is considered as the key pillar of the EU GDPR and also a key means of documenting that your security is up to snuff.

**Ques 43. The EU GDPR compliance mandates that all organizations with access to \_\_\_\_\_\_ of EU citizens take sufficient measures to ensure the security and privacy of their data. Select the appropriate option for the given blank.**

1. Personally Identifiable Information
2. Transferred personal data
3. Data processing contract
4. Subject Access Request

Answer: a) Personally Identifiable Information

Explanation: The EU GDPR compliance mandates that all organizations with access to Personally Identifiable Information of EU citizens take sufficient measures to ensure the security and privacy of their data.

**Ques 44. Regarding data subjects protected by the GDPR, which of the following statements is true?**

1. The GDPR protects only people who are physically located in the EU
2. The GDPR protects only EU citizens
3. The GDPR protects only EU residents
4. The GDPR protects only EU domiciliary

Answer: a) The GDPR protects only people who are physically located in the EU

Explanation: The data protection rules are applicable not only when the controller is established within the EU, but whenever the controller uses equipment situated within the EU in order to process data.

**Ques 45. Consider the example “VA provides the reports from which to validate that appropriate security measures have been implemented and that action has been taken to mitigate vulnerabilities.” Which of the following is the correct option in regards to this statement?**

1. It describes a process for regularly testing
2. It describes the tasks of the data protection officer
3. It describes concept of Activity reports
4. None of these

Answer: b) It describes the tasks of the data protection officer

Explanation: VA provides the reports from which to validate that appropriate security measures have been implemented and that action has been taken to mitigate vulnerabilities. Under Article 39 it is considered under the tasks of the data protection officer.

**Ques 46. A security breach has occurred in an information system that also holds personal data. What is the first thing the controller must do?**

1. Ascertain whether the breach may have resulted in the loss or unlawful processing of personal data.
2. Assess the risk of adverse effects to the data subjects using a privacy impact assessment (PIA).
3. Assess whether personal data of a sensitive nature has or may have been unlawfully processed.
4. Report the breach immediately to the relevant Data Protection Authority.

Answer: a) Ascertain whether the breach may have resulted in the loss or unlawful processing of personal data.

Explanation: The data breach notification obligation as laid down in the Data Protection Act.

**Ques 47. Which of the following is not consider while deploying Vulnerability Assessment to Business Impact in order to comply with the GDPR compliances?**

1. Identify and understand your business processes.
2. Find hidden data sources
3. Determine what hardware underlies applications and data
4. Regularly testing, assessing and evaluating the effectiveness of technical and organizational measures

Answer: d) Regularly testing, assessing and evaluating the effectiveness of technical and organizational measures

Explanation: Regularly testing, assessing and evaluating the effectiveness of technical and organizational measures is described under the GDPR article 32 as the security of processing personal data.

**Ques 48. Which one of the following would be classified as sensitive personal data?**

1. Address
2. CCTV video
3. Name
4. Religion

Answer: d) Religion

Explanation: Sensitive personal data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

**Ques 49. If someone makes a subject access requests (SRAs), within how many days under the GDPR you must respond?**

1. 7
2. 24
3. 30
4. 40

Answer: d) 30

Explanation: Under the DPA, you must respond to SARs within 40 days of receipt of the written request. And, under the GDPR, your organization must respond to SARs within one month of receipt.

**Ques 50. What is the next vulnerability management step you will implement when you understood and mapped out your application and data flows and the underlying hardware, network infrastructure, and protections?**

1. Apply Business and technology context to scanner results
2. Map the network infrastructure that connects the hardware
3. Run vulnerability scans
4. Identify which control is already in place

Answer: c) Run vulnerability scans

Explanation: Only when you’ve understood and mapped out your application and data flows and the underlying hardware, network infrastructure, and protections then you can run your vulnerability scans.

**Ques 51. Binding Corporate Rules are a means for organizations to ease their administrative burden when complying with the GDPR. How do these rules help them?**

1. They allow them to have underpinning contracts with all parties involved abroad.
2. They allow them to let third parties outside the European Economic Area process personal data.
3. They avoid the need to approach each Data Protection Authority in the EU separately.
4. They prevent them from having to ask a DPA for permission for the processing of the data once their BCR are accepted.

Answer: c) They avoid the need to approach each Data Protection Authority in the EU separately.

Explanation: Once BCRs are approved by one DPA inside the EU you don’t have to ask the other DPAs inside the EU to approve them anymore.

**Ques 52. Continuous monitoring will track the status and effectiveness of the measures taken by the controller to mitigate:**

1. Local Add-on Requirements
2. Gap analysis
3. The risk in terms of available technology and costs of implementation
4. Implementation of a data protection structure

Answer: c) the risk in terms of available technology and costs of implementation

Explanation: Continuous monitoring will track the status and effectiveness of the measures taken by the controller to mitigate the risk in terms of available technology and costs of implementation, and/or alternatively that a consultation of the supervisory authority has taken place prior to the processing.

.

**Ques 53. The controller shall implement appropriate technical and organizational measures for ensuring that only personal data which are necessary for each specific purpose of the processing are processed." Which term in the General Data Protection Regulation (GDPR) is defined?**

1. Compliance
2. Data protection by default
3. Data protection by design
4. Embedded protection

Answer: c) Data protection by design

Explanation: By default, the minimum of personal data is to be processed for the shortest possible period, using the best possible security measures to prevent unauthorized access.

**Ques 54. In what condition Continuous Monitoring is considered as more effective?**

1. Where an organization will need to explain their lawful basis for processing the data
2. Where a data protection impact assessment indicates that processing operations involve a high risk
3. Where data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs
4. Where processing of data concerning a natural person's sex life or sexual orientation

Answer: b) Where a data protection impact assessment indicates that processing operations involve a high risk

Explanation: Continuous monitoring is considered more effective in a situation where a data protection impact assessment indicates that processing operations involve a high risk.

**Ques 55. A social services organization plans to design a new database to administrate its clients and the care they need.** **In order to request permission from the Data Protection Authority (DPA), what is one of the first important steps to be taken?**

1. Collect data about the clients and the amount and kind of care needed and provided.
2. Conduct a Privacy Impact Assessment (PIA) to assess the risks of the intended processing.
3. Obtain the consent of the clients for the intended processing of their personal data.

Answer: b) Conduct a Privacy Impact Assessment (PIA) to assess the risks of the intended processing.

Explanation: When asking consent to process data, the data subject 'should be made aware of risks, rules, safeguards, and rights'. So, in order to request permission from the Data Protection Authority (DPA), first conduct a Privacy Impact Assessment (PIA) to assess the risks of the intended processing.

**Ques 56. Which of the following can be used to maintain an enterprise-wide profile of the status of data protection and level of risk with which the organization operates to keeps the required processing information and processes personal data lawfully on an ongoing basis?**

1. The output of a strategically designed and well-managed organization-wide GDPR monitoring program
2. Implementing data minimization, Pseudonymisation, transparency, allowing individuals to monitor processing
3. Implement measures that meet the principles of data protection by design and data protection by default
4. All of these

Answer: a) The output of a strategically designed and well-managed organization-wide GDPR monitoring program

Explanation: The output of a strategically designed and well-managed organization-wide GDPR monitoring program can be used to maintain an enterprise-wide profile of the status of data protection and therefore level of risk with which the organization operates, keeps the required processing information and processes personal data lawfully on an ongoing basis.

**Ques 57. What best describes the principle of data minimization?**

1. Care must be taken to collect as little data as possible in order to protect the privacy and interests of the data subjects.
2. Data must be adequate, relevant and limited to what is necessary for relation to the purposes for which they are processed.
3. In order to keep data manageable, it must be stored in such a manner that it requires a minimal amount of storage.
4. The number of items that are collected per data subject may not exceed the upper limit stated by the Data Protection Authority (DPA).

Answer: b) Data must be adequate, relevant and limited to what is necessary for relation to the purposes for which they are processed.

Explanation: This is the very definition of data minimization (Article 5.1.c). It is aimed at making sure only the data needed to achieve the defined goals are collected.

**Ques 58. A company can present itself as an expert in a specific area of expertise making use of social media. What is the best way to demonstrate expertise in a specific field?**

1. By posting information about the company on Social Media.
2. By actively answering questions on Social Media about their product.
3. By posting about how the product of the competitor is inferior to that of the company.
4. By posting about new products the company is developing.

Answer: b) By actively answering questions on Social Media about their product.

Explanation: Answering (and actively answering) questions about a specific product on social media could make your company an expert.

**Ques 59. In preparing to meet EU GDPR compliance requirements, organizations must observe a minimum set of security controls to avoid both penalties and loss of customer trust. Which of the following is not related to and delivered by Vulnerability Assessment?**

1. Visibility of your IT environment which uncovers blind spots or shadow IT
2. Continuous and automatic updates combined with full remediation capabilities
3. Data processing agreements
4. Reporting with full support for GDPR compliance

Answer: c) Data processing agreements

Explanation: Those related to and delivered by VA include: visibility of your IT environment which uncovers blind spots or shadow IT, continuous and automatic updates combined with full remediation capabilities, asset criticality rankings, reporting with full support for GDPR compliance and integration with your SIEM, ticketing system and other business-critical data.

**Ques 60. What is the purpose of a privacy audit by the supervisory authority?**

1. To fulfill the obligation of the GDPR to implement appropriate technical and organizational measures for data protection.
2. To monitor and enforce the application of the GDPR by assessing that processing is performed in compliance with the GDPR.
3. To advice the controller on the mitigation of privacy risks in order to protect the controller from liability claims for non-compliance to the GDPR.

Answer: b) To monitor and enforce the application of the GDPR by assessing that processing is performed in compliance with the GDPR

Explanation: According to GDPR art 57.1(a) this is an important task of the DPA as supervising authority.

**Ques 61. Where the data subject is a child, what steps must controllers take in respect of consent, within the constraints of available technology?**

1. Controllers must make best efforts to verify the consent
2. Controllers must make reasonable efforts to verify the consent
3. Controllers must make best efforts to request the consent in clear and plain language, in the context of the age of the child
4. Controllers must make reasonable efforts to request the consent in clear and plain language, in the context of the age of the child

Answer: b) Controller must make reasonable efforts to verify the consent.

Explanation: GDPR clearly states that Parental consent will be required for the processing of personal data of children under age 16. The EU Member States may lower the age requiring parental consent to 13.

**Ques 62. While implementing certain data subject rights the controller is NOT obliged by Article 19 to inform each third-party recipient of the personal data" For which of the following rights is that statement TRUE?**

1. "Non-profiling" under Article 22
2. Rectification under Article 16
3. Erasure / "right to be forgotten" under Article 17
4. Restriction under Article 18

Answer: a) "Non-profiling" under Article 22

Explanation: According to Article 22, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her.

**Ques 63. For purposes of a data protection impact assessment, when must the controller seek the views of data subjects or their representatives on the intended processing?**

1. Always
2. Never
3. When appropriate
4. When the supervisory authority requests it

Answer: c) When Appropriate

Explanation: Data controllers will be required to conduct privacy impact assessments where privacy breach risks are high to analyze and minimize the risks to their data subjects.

**Ques 64. Which of the following Article of the GDPR not related to the Vulnerability Assessment?**

1. Article 32
2. Article 57
3. Article 59
4. Article 34

Answer: d) Article 34

Explanation: Article 34 provides provision related to the communication of a personal data breach to the data subject.

**Ques 65. Which of the following is not the requirement mentioned under the provision of Privacy by design and by default?**

1. The amount of the personal data Collected
2. The period of data storage
3. Accessibility of personal data
4. The consent

Answer: d) The consent

Explanation: That obligation of Privacy by design is applied to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility, and, the provision of consent is defined separately under Article 7 of the GDPR.

**Ques 66. “Vulnerability assessments can be invaluable, but only if their results are weighed in the context of the business and existing security infrastructure.” Choose the correct option to justify the given statement.**

1. It shows importance of adding context to security infrastructure
2. Represents importance of scanning vulnerability location
3. Represent implementation of the available security technologies
4. It shows importance of the identification of the vulnerability through scanning

Answer: a) It shows importance of adding context to security infrastructure

Explanations: one of the important steps for effective vulnerability management is adding context which states that Vulnerability assessments can be invaluable, but only if their results are weighed in the context of the business and existing security infrastructure.

**Ques 67. How many principles are there under the Data Protection Act 1998?**

1. 5
2. 8
3. 10
4. 14

Answer: b) 8

Explanation: Anyone holding personal data for other purposes is legally obliged to comply with Data Protection Act 1998, subject to some exemptions. The Act defines eight data protection principles to ensure that information is processed lawfully.

**Ques 68. “BCRs can authorize themselves to make all transfers automatically for all EU members states.” Is this statement true?**

1. Yes
2. No
3. Maybe under Specific circumstances
4. Not sure

Answer: b) No

Explanation: BCRs by themselves do not "authorize" all transfers automatically for all EU member states. Most of the member states still require a formal "transfer notification" which is normally granted if the BCR has been accepted by the relevant country.

**Ques 69. If you lose some personal data, such as on a laptop, who should you report it to?**

1. The Information Commissioner’s office
2. The Health and safety executive
3. The supervisory authority
4. The Government

Answer: c) The supervisory authority

Explanation: if you lose some personal data, such as on a laptop, this is a kind of data breach and the GDPR introduce a duty on all organizations to report certain types of a data breach to the relevant supervisory authority. It will be mandatory to report a personal data breach to the relevant supervisory authority under the GDPR if it is likely to result in a risk to people's rights and freedoms.

**Ques 70. Consider the example “vulnerability found on a server or storage device protected by application firewalls, encryption, and other counter-measures may not be as important to address as the same vulnerability found in a less protected infrastructure used in testing and development, particularly if it makes use of data with stringent compliance requirements.” By which of the following Vulnerability Management step you can handle the given problem.**

1. Available Security Technologies
2. By using existing protection/controls
3. By identifying assets touched by the vulnerability
4. None of these

Answer: b) By using existing protection/controls

Explanation: For addressing vulnerability mention in above example it is important to weigh criticality against existing protections to determine which vulnerability could actually expose your business to serious cyber-attacks.

**Ques 71. Which of the following is NOT true? The Data Protection Act 1998 says that data must be**

1. fairly and lawfully processed
2. un-secure
3. accurate
4. adequate, relevant and not excessive

Answer: b) un-secure

Explanation: The Data Protection Act 1998 says that data must be - fairly and lawfully processed, accurate, adequate, relevant and not excessive. So, the option b) unsecure is not true.

**Ques 72. Under Article 34, communication of personal data breach to the data subject is not required if**

1. It results in a high risk to the rights and freedoms of natural persons
2. The personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons
3. It wouldn’t involve disproportionate effort
4. The controller has implemented appropriate technical and organizational protection measures, which is applied to the personal data affected by the personal data breach

Answer: d) The controller has implemented appropriate technical and organizational protection measures, which is applied to the personal data affected by the personal data breach

Explanation: The communication to the data subject shall not be required if the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular, those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.

**Ques 73. “The controller must implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access.” Under which Article and Recital of the GDPR the data security measures are mentioned.**

1. Recital 82 and Article 31
2. Recital 80 and Article 29
3. Recital 83 and Article 32
4. Recital 73 and Article 45

Answer: c) Recital 83 and Article 32

Explanation: According to Recital 83 and Article 32, Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor, shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

**Ques 74. “The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards”, is mentioned under**

1. Article 49, Derogations for specific situations
2. Article 45, Transfer on the basis of adequacy decision
3. Article 33, Notification of the personal data breach to supervisory authority
4. Article 46, Transfers subjects to Appropriate Safeguards

Answer: a) Article 49, Derogations for specific situation

Explanation: According to Article 49, Transfer or a set of transfers of personal data to a third country or an international organization shall take place when the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

**Ques 75. “The joint controllers are required to enter into a specific arrangement that needs to reflect their roles and relationships toward the data subjects.” Under which article there is a provision of the Joint Controller?**

1. Article24
2. Article 25
3. Article 26
4. Article 32

Answer: c) Article 26

Explanation: Under article 26 of the GDPR, there is the provision of the Joint controller which states where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

**Ques 76. Under which article, in the event of data breach, the data controller is competent to notify the supervisory authority.**

1. Article 43
2. Article 55
3. Article 50
4. Article 45

Answer: b) Article 55

Explanation: In the event of a personal data breach, data controllers must notify the supervisory authority "competent under Article 55" which is most likely the supervisory authority of the member state where the controller has its main establishment or only establishment, although this is not entirely clear.

**Ques 77. Which article provides data controller to show an approved certificate mechanism to demonstrate compliance with the requirements set out in the provision of Data Protection by Design and by Default?**

1. Article 42
2. Article 43
3. Article 49
4. Article 50

Answer: a) Article 42

Explanation: An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out for Privacy by design and by default under Article 25.

**Ques 78. Which of the following statement is not correct about the Binding Corporate Rules?**

1. These are developed to allow personal data transfer between MNCs, international organizations, and groups of companies
2. Developed as an alternative to the U.S. Department of Commerce EU Safe Harbor
3. BCRs can be used as an alternative means of authorizing transfers of personal data within Europe
4. Typically form stringent, intra-corporate global privacy policies, set of practices, processes, and guidelines that satisfy EU standards

Answer: c) Used as an alternative means of authorizing transfers of personal data within Europe

Explanation: BCRs may be available as an alternative means of authorizing transfers of personal data (e.g., customer databases, HR information, etc.) outside of Europe, not only within Europe.

**Ques 79. Under Article 35 of GDPR, there is a provision related to DPIAs, which states that DPIAs help organizations to identify, assess and mitigate or minimize privacy risks with data processing activities. For what DPIA stands for**

1. Data Protection Impact Assessment
2. Data Protection and Investigation Authority
3. Data Providers Investigation Association
4. Data Providers and Investors Association

Answer: a) Data Protection Impact Assessment

Explanation: Data protection impact assessments (DPIAs) help organizations identify assess and mitigate or minimize privacy risks with data processing activities.

**Ques 80. Who is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements, and considered as the mandatory role under Article 37 of the GDPR?**

1. Data Protection Officer (DPO)
2. Data Controller
3. Data Processor
4. None of these

Answer: a) Data Protection Officer (DPO)

Explanation: A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements. When the GDPR becomes effective, the data protection officer becomes a mandatory role under Article 37 for all companies that collect or process EU citizens’ personal data.