### Exam for the GDPR Foundation

(Multiple Choice)

**Ques 1. 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 2. In order to embed privacy in the design process, several aspects must be taken into consideration. Which one of them is not considered to embed privacy in design?**

1. Operate within legal boundaries and be accountable
2. Organization should determine how transparent it wants to be in its data processing
3. Communication towards data subjects is not important
4. None of these

Answer: c) Communication to data subjects is not important

Explanation: Communication towards data subjects is very important to address at the initial design stages and throughout the complete development process. Communication lines must be clear, also when something goes wrong. For data subjects, it must be clear where they can turn if they want to know more about the processing of their personal data and how they can exercise their rights.

**Ques 3. Pseudonymized data can “no longer be attributed to a specific data subject without the use of additional information” according to GDPR legislation. What does it mean?**

1. You need to limit the potential exposure and pseudonymize the data
2. You require potentially lots of testing
3. You don’t need to access personal data
4. I don’t know

Answer: a) You need to limit the potential exposure and pseudonymize the data

Explanation: According to GDPR legislation, data which is Pseudonymized can no longer be attributed to a specific data subject without the use of additional information, it implies that you need to limit the potential exposure and pseudonymize the data.

**Ques 4. The official name of Data Protection Impact Assessment is**, **Analyse d'Impact Relative à la Protection des Données (APID), in which language.**

1. Spanish
2. French
3. Italian
4. Irish

Answer: b) French

Explanation: DPIA documents are in French. The French official name for **Data Protection Impact Assessment (DPIA**) is **Analyse d'Impact Relative à la Protection des Données**, also known as **AIPD**).

**Ques 5. What is the GDPR mainly intended for?**

1. To be a common ground upon which the member states can build their own laws.
2. To make non-EU countries respect the right to privacy of individuals within the EU.
3. To secure privacy as a fundamental human right for everyone.
4. To strengthen and unify data protection for individuals within the EU.

Answer: d) To strengthen and unify data protection for individuals within the EU.

Explanation: The scope of the GDPR is limited to data protection as a right of individuals within the EU and aims to harmonize the rules for that within the EU.

**Ques 6. Under GDPR data controllers are required to inform/notify about the data breach to**

1. Supervisory Authority
2. Affected Data Subjects
3. All Data Subject
4. Both (a) and (b)
5. All of the above

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

Explanation: The GDPR defines that if an organization faces breach then it is required to inform to both the supervisory authority and affected data subjects.

**Ques 7. Under which Article GDPR provide provision related to sensitive personal data as “special categories of personal data.”**

1. Article 9 c) Article 43
2. Article 20 d) Article 6

Answer: a) Article 9

Explanation: Under Article 9 of GDPR there is a provision related to Processing of special categories of personal data. It states that “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.”

**Ques 8. GDPR applies to -**

1. Processors only c) Both the processor and controller
2. Controller only d) None of these

Answer: c) Both the Controller and the Processor

Explanation: The GDPR applies to both the controllers **and** processors. It is the responsibility of the controller to determine the purposes and means of processing personal data, while the processor is responsible for processing personal data on behalf of a controller.

**Ques 9. What happens when a profiling data subject requests the halt of the profiling?**

1. The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information
2. The processing must cease unless the controller demonstrates that the objection overrides the interests, rights, and freedoms of the data subject
3. Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, etc.
4. Any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis

Answer: b) The processing must cease unless the controller demonstrates that the objection overrides the interests, Rights, and freedoms of the data subject

Explanation: Under Article 19, upon the data subject’s request to halt the profiling, the processing must cease unless the controller demonstrates that the objection overrides the interests, rights, and freedoms of the data subject.

**Ques 10. Under which article provision of Transfers of personal data to third countries or international organizations is not mention.**

1. Article 45 c) Article 44
2. Article 43 d) Article 49

Answer: b) Article 43

Explanation: Article 43 deals with the responsibilities of the Controllers and the Processors. While under chapter 5 which contains article 44 to article 50 define provisions regarding the transfer of personal data to third countries or international organizations.

**Ques 11. What is new in GDPR?**

1. Introduces new rights for people to access the information that companies hold about them.
2. Defines a mandatory provision of disclosure of the Data Breach.
3. Fines are increased up to 4% of the global turnover.
4. All of the Above

Answer: d) All of the above

Explanation: GDPR introduces new rights for people to access the information that companies hold about them. GDPR provides individual more control over the processing of their personal data, with new and enhanced rights, which includes right to data portability, right not to be subject to a decision based on profiling, etc. it also defines a mandatory provision of disclosure of the Data Breach without undue delay or within the 72 hours, after first becoming aware of a data breach. GDPR also provides supervisory authorities to enforces serious fines like fines of 4% of the total worldwide annual turnover of the foregoing financial year.

**Ques 12. “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 13. In essence, companies will now be obliged to take into account data privacy during design stages of all projects along with the lifecycle of the relevant data process. What this obligation specifically called?**

1. Privacy law
2. Privacy by design
3. Enterprise data privacy
4. Privacy protection law

Answer: b) Privacy by Design

Explanation: The GDPR defines many key changes one of them is Privacy by Design which obliged organizations to take into account data privacy during design stages of all projects along with the lifecycle of the relevant data process.

**Ques 14. “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 15. DPIA is always required for:**

1. When private data is collected from third parties and the data is used to decide whether to allow or deny access to a service
2. Processing of data related exclusively to administration of personnel of an organization if the data is unrelated to health of the data subject
3. Processing of data related only to administration of salaries
4. If data is processed only and exclusively to register visitors, as part of access control

Answer: a) When private data is collected from third parties and the data is used to decide whether to allow or deny access to a service

Explanation: DPIA always necessary for conditions such as when private data is collected from third parties and the data is used to decide whether to allow or deny access to a service, e.g. automatic decision making, if there is a need to assess and process private personal aspects, etc.

**Ques 16. Which of the following Regulation is based on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC Privacy of EU citizens?**

1. Data Protection Directive c) Privacy Act
2. General Data Protection Regulation d) Online Privacy Protection Act

Answer: b) General Data Protection Regulation (GDPR)

Explanation: GDPR is the Act introduced to strengthen and unify data protection for all individuals within the European Union (EU) and provides protection to the export of personal data outside the EU.

**Ques 17. A GDPR is a one-stop shop. What does one-stop shop mean?**

1. Firms will only have to deal with a single supervisory authority, not one for each of the EU’s 28-member states.
2. Public authorities and employers will need to take extra care to show that consent is freely given and should avoid over-reliance on consent.
3. Greater freedom is accompanied by the Controller’s obligation to demonstrate the reasons that led to the adoption of a specific decision, as well as to document those choices.
4. All of the above

Answer: a) A new one-stop shop for businesses means that firms will only have to deal with a single supervisory authority, not one for each of the EU’s 28-member states

Explanation: A new one-stop shop for businesses means that firms will only have to deal with a single supervisory authority, not one for each of the EU’s 28-member states, making it simpler and cheaper for companies to do business in the EU. This will also have a positive impact on Internet service providers with offices in several EU countries.

**Ques 18. The General Data Protection Regulation (GDPR) is related to personal data protection. What is the definition of personal data?**

1. Any information relating to an identified or identifiable natural person.
2. Any information that the European citizens would like to protect.
3. Data that directly or indirectly reveal someone's racial or ethnic background, religious views, and data related to health or sexual habits.
4. Preservation of confidentiality, integrity and availability of information.

Answer: a) Any information relating to an identified or identifiable natural person.

Explanation: According to official definition under the GDPR the personal data is any information relating to an identified or identifiable natural person.

**Ques 19. Is process of profiling is also applicable to children?**

1. Yes, children are included under profiling
2. Yes, but under specific circumstances
3. No
4. I don’t know

Answer: c) No

Explanation: No, profiling and automated decision-making are not allowed on children, irrespective of their age.

**Ques 20. “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 21. According to the General Data Protection Regulation (GDPR), what is the definition of 'processing' of personal data?**

1. Any operation that can be performed on personal data.
2. Any operation that can be performed on personal data, except erasing and destroying.
3. Only operations in which the data is being shared on social media or transferred by email or otherwise through the Internet.
4. Only operations in which the personal data is used for the purposes for which it was collected.

Answer: a) Any operation that can be performed on personal data.

Explanation: according to the GDPR, the definition of processing of personal data is an action that is performed on personal data or sets of data.

**Ques 22. The GDPR defines Pseudonymisation as**

1. Spanish
2. A process that transforms personal data in such a way as it cannot be attributed to a real person.
3. Italian
4. Irish

Answer: b) Pseudonymisation is a process that transforms personal data in such a way as it cannot be attributed to a real person.

Explanation: GDPR refers to Pseudonymisation as a process that transforms personal data in such a way as it cannot be attributed to a real person.

**Ques 23. 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 24. Who is responsible to help in identifying the key persons, and to assist in the process of conducting of DPIA?**

1. Application Developers
2. Data Vendors
3. Data Protection Officer
4. Project Managers

Answer: c) Data Protection Officer

Explanation: It is the Data Protection Officer’s (DPO) duty to help in identifying the key persons, and to assist in the process of conducting of DPIA (however, DPO does not necessarily need to be the one who actually conducts a DPIA).

**Ques 25. What is new in the GDPR?**

1. It introduces new rights for people to access the information that companies hold about them.
2. It introduces a new right to Data Portability.
3. It defines a mandatory provision of disclosure of the Data Breach.
4. Fines are increased up to 4% of the global turnover.
5. All of the Above

Answer: e) All of the Above

Explanation: The GDPR introduces new rights for people to access the information companies’ hold about them, obligations for better data management for businesses, and a new regime of fines.

**Ques 26. Which organizations are not strictly bounded to follow the GDPR Compliances?**

1. Organizations dealing with the personal data of the EU citizens
2. Those organizations which are not physically located within EU but providing services to EU states.
3. Organizations with fewer than 250 employees
4. None of the above

Answer: c) Organization with fewer than 250 employees

Explanation: The GDPR does recognize that smaller businesses require different treatment compared to larger enterprises. Article 30 of the regulation states that organizations with **fewer than 250 employees** will not be as strictly bound by GDPR.

**Ques 27. Under which circumstances the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the Regulation?**

1. When processing of personal data relating to criminal convictions and offenses
2. When children data is being processed by the controller
3. If there is a processing of the special category of the personal data
4. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller

Answer: d) If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller

Explanation: Under Article 11 of the GDPR, If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

**Ques 28. Which of the following provision is mentioned in the Article 25 of the GDPR?**

1. Data Protection by Design and by Default
2. Cooperation with the Supervisory Authority
3. Records of Processing Activities
4. Processing under the authority of the controller or the processor

Answer: a) Data Protection by Design and by Default

Explanation: The article 25 of the GDPR specifies the Data protection by design and by default.

**Ques 29. 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 30. Does Data Controller have the freedom to choose methodology required for the DPIA?**

1. Yes
2. No
3. Yes, but under some obligations
4. I don’t know

Answer: a) Yes, under some obligations

Explanation: There is a freedom of choice when it comes DPIA methodology. The responsibility of choosing a methodology is in the hands of the data controller (organization, company). But the **DPIA methodology used in practice can and should be adapted to particular circumstances, needs and requirements.**

**Ques 31. A common characteristic of a DPIA doesn’t include:**

1. Definition of acceptable risk values
2. Tools of effectiveness
3. Specification of risk assessment criteria for the rights and freedoms of natural persons
4. Identification of appropriate risk mitigation measures

Answer: b) Tools of Effectiveness

Explanation: Tools of Effectiveness, as audit, training, complaint handling system, etc. are considered under BCRs. While Context definition (internal and external factor), Specification of risk assessment criteria for the rights and freedoms of natural persons, Identification, and analysis of risks, Definition of acceptable risk values and Identification of appropriate risk mitigation measures are some common characteristics of the DPIAs.

**Ques 32. What is Pseudonymous data?**

1. Personal data that has been subjected to technological measures (like hashing or encryption) such that it no longer directly identifies an individual without the use of additional information.
2. Data in an encrypted form
3. Personal data stored by the Data controllers
4. None of these

Answer: a) Pseudonymous data is defined as the personal data that has been subjected to technological measures (like hashing or encryption) such that it no longer directly identifies an individual without the use of additional information.

Explanation: Pseudonymous data are still treated as personal data because they enable the identification of individuals. The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

**Ques 33. Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility. Which of the following information is not correct about the record of processing?**

1. The name and contact details of the controller and, where applicable, the joint controller, the controller’s representative and the data protection officer
2. It doesn’t specify description of the categories of data subjects and of the categories of personal data
3. It describes the purposes of the processing
4. All of the above

Answer: b) It doesn’t specify description of the categories of data subjects and of the categories of personal data

Explanation: Under Article 30, the record of processing shall include the information like a description of the categories of data subjects and of the categories of personal data; the purposes of the processing; name and contact details of the controller, etc.

**Ques 34. 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 35. Under which circumstances the data controller is not obligated to provide the breach notice to the supervisory authority**.

1. If the controller provides a reasoned justification for the data breach
2. If controller became aware of the breach and deal with it
3. If the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons
4. None of these as under all circumstances controller is mandated to provide breach notification

Answer: c) If the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons

Explanation: Article 33(1) contains a key exception to the supervisory authority notification requirement: Notice is not required if “the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons.”

**Ques 36. “Individuals also have the right to demand that their data is deleted if it's no longer necessary to the purpose for which it was collected.” This statement is defined under which of the Individual right provided by GDPR.**

1. Right to data Correction c) Right to Forgotten
2. Right to restrict processing d) Right to Data Portability

Answer: C) Right to Forgotten

Explanation: Individuals also have the right to demand that their data is deleted if it is no longer necessary to the purpose for which it was collected. This is known as the 'right to be forgotten'. Under this rule, they can also demand that their data is erased if they have withdrawn their consent for their data to be collected, or object to the way it is being processed.

**Ques 37. “Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment.” as a Right to an effective judicial remedy against a controller or processor is mentioned under which article of the GDPR?**

1. Article 75 c) Article 77
2. Article 79 d) Article 80

Answer: b) Article 79

Explanation: Under Article 79 provision of a Right to an effective judicial remedy against a controller or processor is given. It states that Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

**Ques 38. Is it important for the Data Controller to provide Data Subjects information necessary to ensure fair and transparent processing in respect of the data subject like the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period?**

1. Yes, it is important
2. Not so important
3. Only if Data Subject asks
4. Not Sure

Answer: a) Yes, it is important

Explanation: The controller, under Article 14 mandates to provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

**Ques 39. Which of the following obligation is the Joint Controller not mandated to?**

1. The responsibility for providing clear information to data subjects
2. **Each joint controller is not liable for the entirety of the damage**, although national law may apportion liability between them
3. Some joint controllers may find themselves facing much higher liability for claims made under the GDPR
4. All of these

Answer: b) **Each joint controller is not liable for the entirety of the damage**, although the national law may apportion liability between him and her.

Explanation: According to **Article 26(3) of GDPR,** Data subjects are entitled to enforce their rights against any of the joint controllers. **Each joint controller is liable for the entirety of the damage**, although the national law may apportion liability between him and her.

**Ques 40. 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 41. 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 42. 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.

**Ques 43. 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. When the supervisory authority requests it c) Never
2. Always d) When Appropriate

Answer: d) 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 44. Where personal data not obtained from the data subject, who is responsible for providing data subjects with the information like the identity and the contact details of the controller, the contact details of the data protection officer, etc.?**

1. Data Protection Officer c) Data Controller
2. Either (a) or (b) d) Not sure

Answer: c) Data Controller

Explanation: According to Article 14 of the GDPR, where personal data have not been obtained from the data subject, the controller shall provide the data subject with the information like the identity and the contact details of the controller and, where applicable, of the controller’s representative; the contact details of the data protection officer, where applicable; etc.

**Ques 45. 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 46. “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 47. GDPR applies to which types of individuals or organizations –**

1. Any organization that processes personal data
2. All data controllers and processors established in the EU and organizations that target EU citizens
3. Data controllers operating in the EU

Answer: b) All data controllers and processors established in the EU and organizations that target EU citizens

Explanation: The GDPR regulation applies to both controllers and processors of data. The GDPR applies to processing carried out by organizations operating within the EU. It also applies to organizations outside the EU that offer goods or services to individuals in the EU.

**Ques 48. Which of the following statement is correct about the Data Protection Officers?**

1. EU institutions and bodies expressly provide that the DPO shall receive any instructions regarding the performance of her duties
2. The DPO should be an employee on a short or fixed term contract
3. The DPO should be a controller of processing activities
4. The DPO should have the authority to investigate

Answer: d) The DPO should have the authority to investigate

Explanation: The GDPR compliances provide DPO the authority to investigate. In EU institutions and bodies, for instance, DPOs have immediate access to all personal data and data processing operations; those in charge are also required to provide information in reply to her questions.

**Ques 49. What is the maximum data breach penalty, under the GDPR compliance directives?**

1. 20,000,000 euros or up to 4% of annual turnover, whichever is greater
2. 10,000,000 euros or up to 2% of annual turnover, whichever is greater
3. There is no maximum fine

Answer: a) 20,000,000 euros or up to 4% of annual turnover, whichever is greater

Explanation: In the case of non-compliance with key provisions of the GDPR or data breach, regulators have the authority to collect a fine in an amount that is up to the greater of €20 million or 4% of global annual revenue in the prior year.

**Ques 50. In which of the following condition Article 6 of GDPR: The Lawfulness of Processing Personal Data is not applied.**

1. The data subject has given consent to the processing of his or her personal data for one or more specific purposes
2. Processing is necessary in order to protect the vital interests of the data subject or of another natural person
3. Processing is necessary for compliance with a legal obligation to which the controller is subject
4. None of these

Answer: d) None of these

Explanation: Here option (d) is correct because when all the remaining three options are considered under the Lawfulness of Processing.

**Ques 51. "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 52. The text of the new Regulation on Personal Data Protection contains explicit references to the concept of “accountability.” What does Accountability stand for?**

1. It refers to an increased territorial scope – it applies to **all companies** that process personal data of people residing in the union, regardless of the company’s location.
2. The concept of “accountability” specifies that the Data Controller should implement (as well as review and update) adequate technical and organizational measures to ensure and be able to demonstrate that the processing operations are carried out according to the new rules.
3. Data processing at any time, and it must be easy for them to do so and provide more control to the data subjects.
4. All of the above

Answer: B) The concept of “accountability” specifies that the Data Controller should implement (as well as review and update) adequate technical and organizational measures to ensure and be able to demonstrate that the processing operations are carried out according to the new rules.

Explanation: In Art 24 of the Regulation, the concept of Accountability is given and is partially included in the Art 29 Data Protection Working Party in Opinion no. 3/2010. The concept of Accountability specifies that the Data Controller should implement (as well as review and update) adequate technical and organizational measures to ensure and be able to demonstrate that the processing operations are carried out according to the new rules. The measures to be adopted have to be evaluated on a case-by-case basis, taking into account a number of factors including the nature, scope, context, and purpose of the processing.

**Ques 53. In May 2018, GDPR regulations will give EU residents and citizens more rights and control over their data. However, in what terms will they have more rights and control?**

1. The right to be forgotten (right to erasure)
2. The right of data portability
3. Both A and B
4. None of the Above

Answer: c) Both A and B

Explanation: GDPR regulations will give EU residents and citizens more rights and control over their data. GDPR provides 8 main rights for individuals and strengthens those that already exist under the current Data Protection Act. The rights of the individuals include - The right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and, rights related to automated decision making and profiling.

**Ques 54. “The Recitals are essential to your understanding the General Data Protection Regulation.” How many recitals are there in the GDPR compliance?**

1. 174 c) 182
2. 176 d)173

Answer: d) 173 Recitals

Explanation: The GDPR text is lengthy and comprises 99 Articles and 173 Recitals.

**Ques 55. Within what period of time must an organization notify a supervising authority about a data breach?**

1. Within 48 hours
2. Within 12 hours
3. Within 72 hours
4. Within 24 hours

Answer: c) Within 72 hours

Explanation: In GDPR it is mandatory for an organization to provide breach notification to a supervisory authority within 72 hours. It is mandatory for all members within the state and requires that the company must notify their customers, the controllers, without undue delay or within the 72 hours, after first becoming aware of a data breach.

**Ques 56. The \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ must be exclusive, reflective of a data subject’s discretionary action, a positive and freely given response to the well-structured, unambiguous description of the processing activity.**

1. Right to privacy c) Acknowledgement
2. Consent d) Processing

Answer: b) Consent

Explanation: Consent must be exclusive, reflective of a data subject’s discretionary action, a positive and freely given response to the well-structured, unambiguous description of the processing activity. The principle of opt-in is obligatory, meaning no processing can take place until consent is assured.

**Ques 57. Which of the following companies/Company have not obtained authorizations for BCRs:**

1. Intel Corporation
2. Motorola Solutions, Inc.
3. HP Enterprise
4. None of these

Answer: d) None of these

Explanation: All companies mentioned above have already obtained authorizations for BCRs.

**Ques 58. When will the European Data Protection Regulation (GDPR) be applicable in all member states to harmonize data privacy laws across Europe?**

1. June 25,2018 c) April 25, 2018
2. February 25, 2018 d) May 25, 2018

Answer: d) May 25, 2018.

Explanation: This Regulation was adopted on 27 April 2016, and it becomes enforceable from 25 May 2018 after a two-year transition period.

**Ques 59. Data held in an encrypted or pseudonymised form is not deemed to be personal data.**

1. True
2. False

Answer: a) True

Explanation: Under the GDPR the Data held in an encrypted or pseudonymised form isn’t deemed to be personal data.

**Ques 60. The GDPR's protection of EU citizens' data only applies to companies located in Europe.**

1. True
2. False

Answer: b) False

Explanation: GPDR makes its applicability very clear – it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU.

**Ques 61. The GDPR requires all businesses to designate a Data Protection Officer (DPO).**

1. True
2. False

Answer: b) False

Explanation: DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large-scale systematic monitoring, or (c) organizations that engage in large-scale processing of sensitive personal data (Art. 37). If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO.

**Ques 62. Personal data that is ‘pseudonymized’ or securely encrypted in some way for purposes of enhanced data protection will be treated in exactly the same way as standard, unmodified personal data under the GDPR.**

1. MYTH
2. FACT

Answer: b) FACT

Explanation: Pseudonymized or encrypted data will benefit from some conditional relaxations under the GDPR in terms of data breaches if it is not deemed to pose significant risk. However, for the most part, such data will be subject to the same data protection rules as ordinary data.

**Ques 63.** The GDPR does not include any changes to the provisions for consent from the previous 1995 Data Protection Directive, currently in effect.

1. True
2. False

Answer: b) False

Explanation: The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

**Ques 64. Under the GDPR, EU citizens can have their data erased permanently and not shared.**

1. True
2. False

Answer: a) True

Explanation: Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

**Ques 65. Demonstrating compliance with the regulation requires:**

1. Implementing technical and organisational measures that ensure and demonstrate you comply
2. Maintain documentation on processing activities
3. In certain circumstances (public sector, systematic/mass processors) appoint a DPO.
4. All of the above

Answer: d) All of the above

Explanation: To demonstrate compliance, the GDPR requires that technical and organisational measures are implemented, documentation on processing activities is maintained and requires that a DPO is appointed where necessary.

**Ques 66. When presented with a list of social issues facing people in the UK today were people more concerned about ‘protecting people’s personal information’ or ‘protecting freedom of speech’?**

1. protecting people’s personal information
2. protecting freedom of speech

Answer: a) protecting people’s personal information

Explanation: More people were concerned about Protecting people’s personal information (22%), than protecting freedom of speech (13%)

**Ques 67. Once the GDPR is introduced, individuals will receive a new ‘right to be forgotten’. This means that organizations can effectively only process their personal data for as long as this data remains necessary for the original purpose for which it was collected.**

1. MYTH – Individuals will not have any absolute right to be forgotten under the GDPR unless they clearly stipulate that they only wish for their data to be used for one singular purpose at the point that data is collected. If individuals wish for their data to be ‘forgotten’ by an organization at a later date, they can only do so by exercising their right to restrict processing by contacting the company.
2. FACT – Individuals will have an absolute right to be forgotten under the new rules of the GDPR.

Answer: b) FACT

Explanation: Individuals will have an absolute right to be forgotten under the new rules of the GDPR.

**Ques 68. The GDPR is a piece of European Union (EU) legislation and therefore theoretically will only be implemented in the UK from 25 May 2018 onwards if this is agreed during ongoing Brexit negotiations.**

1. FACT – The GDPR is strictly a piece of EU legislation and, due to the Repeal Bill, will not form part of UK legislation unless decided otherwise during Brexit negotiations.
2. MYTH – Although the GDPR is a piece of EU legislation, it will form part of UK legislation from 25 May 2018 onwards regardless of the UK’s position in terms of Brexit negotiations at that time.

Answer: b) MYTH

Explanation: Although the GDPR is a piece of EU legislation, it will form part of UK legislation from 25 May 2018 onwards regardless of the UK’s position in terms of Brexit negotiations at that time.

**Ques 69. 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 70. According to the General Data Protection Regulation (GDPR), which personal data category is regarded as sensitive data?**

1. Credit card details
2. Trade union membership
3. Passport number
4. Social security number

Answer: b) Trade union membership

Explanation: According to the General Data Protection Regulation (GDPR), membership of a trade union is sensitive data.

**Ques 71. The processing of personal data has to meet general rules on quality. What is one of these rules defined by the GDPR?**

1. The data processed must be archived.
2. The data processed must be encrypted.
3. The data processed must be indexed.
4. The data processed must be relevant.

Answer: d) The data processed must be relevant.

Explanation: The data processed must be relevant and this requirement is defined by the GDPR.

**Ques 72. Every time personal data is processed, proportionality and subsidiarity must be checked. What is the requirement for the personal data being processed?**

1. It must be limited always to what is necessary to achieve the defined goals and must be limited to the least “intrusive” data.
2. It must be handled by the smallest number of employees possible and they must work for the Controller or an affiliate.
3. It must be limited to a predefined storage size and the system used must be financed by the Controller.
4. It must be used for the smallest number of purposes possible and this may not be done outside the premises of the Processor.

Answer: a) It must be limited always to what is necessary to achieve the defined goals and must be limited to the least “intrusive” data.

Explanation: These terms mean you collect no more data than needed to achieve the predefined goal(s), and you always try to use data that has the least impact on the privacy of the Data Subject.

**Ques 73. What is the term used in the General Data Protection Regulation (GDPR) for unauthorized disclosure of, or access to, personal data?**

1. confidentiality violation
2. data breach
3. incident
4. security incident

Answer: b) data breach

Explanation: The term used in the General Data Protection Regulation (GDPR) for unauthorized disclosure of, or access to, personal data is data breach. The GDPR introduces a duty on all organizations to report certain types of data breach to the relevant supervisory authority. In some cases, organizations will also have to report certain types of data breach to the individuals affected.

**Ques 74. While performing a backup, a data server disk crashes. Both the data and the backup are lost. The disk contained personal data but no sensitive data. What kind of incident is this?**

1. data breach
2. security breach
3. security incident

Answer: a) data breach

Explanation: Personal data irretrievably lost is regarded as unauthorized processing, which makes it a data breach under the GDPR.

**Ques 75. Data Protection Authorities are assigned a number of responsibilities aimed at making sure Data Protection Regulations are complied with. What is one of those responsibilities?**

1. Assessing codes of conduct for specific sectors relating to the processing of personal data.
2. Defining a minimum set of measures to be taken to protect personal data.
3. Investigation of all data breaches of which they have been notified.
4. Review of contracts and BCRs on compliance with the regulations.

Answer: a) Assessing codes of conduct for specific sectors relating to the processing of personal data.

Explanation: One of the responsibilities of DPAs is to provide general advice on how to comply with the regulations.

**Ques 76. 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 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 with the relevant Data Protection Authority.

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

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

**Ques 77. Which right of Data Subjects is explicitly defined by the GDPR?**

1. A copy of personal data must be provided in the format requested by the Data Subject.
2. Access to personal data without any cost for the Data Subject.
3. Personal data must be always changed at the request of the Data Subject.
4. Personal data must be erased at all times if a Data Subject requests this.

Answer: b) Access to personal data without any cost for the Data Subject.

Explanation: However only the first copy has to be provided free of cost but this right of Data Subjects is explicitly defined by the GDPR.

**Ques 78. The GDPR distinguishes 'sensitive personal data' as a special category of personal data. What is an example of such data?**

1. an appointment in a hospital with a medical specialist
2. an International Bank Account Number (IBAN)
3. subscription to a scientific journal for politics
4. the membership of a branch association

Answer: a) an appointment in a hospital with a medical specialist

Explanation: An appointment with a medical specialist is 'personal data concerning health.

**Ques 79. Which role in data protection determines the purposes and means of the processing of personal data?**

1. Controller
2. Data Protection Officer
3. Processor

Answer: a) Controller

Explanation: Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data and determines which equipment can be used.

**Ques 80.** Which information is regarded as personal data according to the General Data Protection Regulation (GDPR)?

1. information about a person, which might harm the privacy of that person, even when untrue
2. any information regarding an identifiable natural person
3. information, regarding an identifiable natural person, which is digitalized

Answer: b) any information regarding an identifiable natural person

Explanation: "Personal data" under the GDPR shall mean any information relating to an identified or identifiable natural person ("data subject").