**Under GDPR data controllers are required to inform/notify about the data breach to -**

1. Supervisory Authority. *This answer is incorrect because under the GDPR it is mandatory that if an organization faces any data breach then the data controllers need to inform to both the supervisory authority and affected data subjects.*
2. Affected Data Subjects. *This answer is incorrect because the GDPR defines that if an organization faces any data breach then not only affected data subjects but supervisory authorities must be notified.*
3. All Data Subject. *This answer is incorrect because the GDPR defines that if an organization faces breach then all data subjects not need to be informed but only the affected data subjects and supervisory authority.*
4. Supervisory Authority & Affected Data Subjects. *This answer is correct because the GDPR defines that if an organization faces breach then it is required to inform to both the supervisory authority and affected data subjects.*

Answer: d) Supervisory Authority & Affected Data Subjects.

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

1. a) Within 48 hours. *This answer is incorrect because under the GDPR it is mandatory for an organization to provide breach notification to a supervisory authority within 72 hours.*
2. b) Within 12 hours. *This answer is incorrect because in GDPR the supervisory authority must be notified about a data breach within 72 hours.*
3. c) Within 72 hours. *This answer is correct because 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.*
4. d) Within 24 hours. *This answer is incorrect because under the GDPR an organization must provide breach notification to a supervisory authority within 72 hours.*

Answer: c) Within 72 hours

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

1. confidentiality violation. *This answer is incorrect because the term used in the General Data Protection Regulation (GDPR) for unauthorized disclosure of, or access to, personal data is data breach.*
2. data breach. *This answer is correct because 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.*
3. incident. *This answer is incorrect because the term used under the new General Data Protection Regulation (GDPR) regulation for unauthorized disclosure of, or access to, personal data is data breach.*
4. security incident. *This answer is incorrect because data breach is the term used in the General Data Protection Regulation (GDPR) for unauthorized disclosure of, or access to, personal data breach.*

Answer: b) data breach

**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. *This answer is correct because personal data irretrievably lost is regarded as unauthorized processing, which makes it a data breach under the GDPR*.
2. security breach. *This answer is incorrect because it’s a kind of unauthorized processing due to personal data lost, and unauthorized processing under the GDPR is termed as data breach.*
3. security incident. *This answer is incorrect because it’s a kind of unauthorized processing due to personal data lost, so this incident is known as data breach under the GDPR.*
4. Incident. *This answer is incorrect because it’s a kind of unauthorized processing due to personal data lost, so this type of security breach is known as data breach under the GDPR.*

Answer: a) data breach

**GDPR doesn’t require data controllers and processors to designate a DPO in a case where:**

1. The processing is carried out by a public authority or body. *This answer is incorrect because GDPR require data controllers and processors to designate a DPO if the processing is carried out by a public authority.*
2. The processing is carried out by a supervisory authority. *This answer is correct because GDPR doesn’t require data controllers and processors to designate a DPO if the processing is carried out by a supervisory authority.*
3. The ‘core activities’ of the data controller/processor consist of processing operations which ‘require regular and systematic monitoring of data subjects on a large scale’. *This answer is incorrect because the GDPR require data controllers and processors to designate a DPO if the ‘core activities’ of the data controllers and processors consist of processing operations which ‘require regular and systematic monitoring of data subjects on a large scale’.*
4. The core activities of the controller/processor consist of processing on a large scale of ‘special categories of data’ or personal data relating to criminal convictions and offences. *This answer is incorrect because GDPR require data controllers and processors to designate a DPO if the core activities of the controller/processor consist of processing on a large scale of ‘special categories of data’ or personal data relating to criminal convictions and offences.*

Answer: b) The processing is carried out by a supervisory authority.