**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. *This answer is correct because one of the responsibilities of DPAs is to provide general advice on how to comply with the regulations.*
2. Defining a minimum set of measures to be taken to protect personal data. *This answer is incorrect because a DPA will give general advice on what they consider an appropriate level of security. They will however not tell you what specific measures you need to take to achieve that level. Even if they want to they would not be able to, because there simply is no one-size-fits-all solution.*
3. Investigation of all data breaches of which they have been notified. *This answer is incorrect because DPAs don’t have the obligation, nor the capacity to investigate all breaches they know of. But they will investigate those they deem significant or noteworthy.*
4. Review of contracts and BCRs on compliance with the regulations. *This answer is incorrect because a DPA is not a legal council. They don’t review contracts or Binding Corporate Rules. However, in the course of an investigation they might take a look at a specific contract or set of BCRs.*

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

**“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. *This answer is incorrect because under this rule the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.*
2. Right to Forgotten. *This answer is correct because individuals 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 Under this rule, they can also demand that their data is erased if they have withdrawn their consent for their data to be collected, or object to the way it is being processed.*
3. Right to restrict processing. *This answer is incorrect because under this rule the data subject shall have the right to obtain from the controller restriction of processing.*
4. Right to Data Portability. *This answer is incorrect because under this rule the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.*

Answer: b) Right to Forgotten

**What is Pseudonymous data?**

1. Personal data that has been subjected to technological measures such that it no longer directly identifies an individual without the use of additional information. *This answer is correct because 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 is known as pseudonymous data. The pseudonymous data are still treated as personal data because they enable the identification of individuals.*
2. Data in an encrypted form. *This answer is incorrect because data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Data in an encrypted form is commonly referred to as ciphertext.*
3. Personal data stored by the Data controllers. *This answer is incorrect because personal data stored by the data controllers are data which relate to a living individual who can be identified from those data.*
4. None of these. *This answer is incorrect because pseudonymous data is defined as the personal data that has been subjected to technological measures such that it no longer directly identifies an individual without the use of additional information.*

Answer: a) Personal data that has been subjected to technological measures such that it no longer directly identifies an individual without the use of additional information.

**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). *This answer is incorrect because GDPR regulation provides EU residents and citizens more rights and control. Under this rule, individuals have the right to demand that their data is deleted if it is no longer necessary to the purpose for which it was collected.*
2. The right of data portability. *This answer is incorrect because under this rule the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.*
3. Both A and B. *This answer is correct because 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.*
4. None of the Above. *This answer is incorrect because GDPR regulations will give EU residents and citizens more rights and control over their data by providing 8 main rights of individuals, in which right to be forgotten and right of data portability is included. So, the correct answer is both a and b.*

Answer: c) Both A and B

**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 Officer (DPO). *This answer is incorrect because data protection officers (DPOs) are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.*
2. the manager of the department. *This answer is incorrect because according to the general data protection regulation data breach of sensitive personal data must be reported to the Data Protection Authority.*
3. the police. *This answer is incorrect because under the GDPR, data breaches must be reported to the Data Protection Authority.*
4. the Data Protection Authority (DPA). *This answer is correct because 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.*

Answer: d) the Data Protection Authority (DPA)