

Exam : **PDPF**

Title : Privacy and Data Protection
Foundation Exam

Version : DEMO

1.What is the essence of the principle 'Full Lifecycle Protection'?

- A. Delivering the maximum degree of data protection by default, ensuring that personal data are automatically protected in any given IT system or business practice.
- B. Ensuring that whatever business practice or technology is involved, processing is done according to the stated objectives, subject to independent verification.
- C. Embedding security measures to protect the data from the moment it is collected, throughout processing until it is destroyed at the end of the process.
- D. Prioritizing the protection of the interests of the individual by offering for example strong privacy defaults, appropriate notice or empowering user-friendly options.

Answer: C

2.A processor is instructed to report on customers who bought a product both last month and at least once in the three months before that. Unfortunately, the processor makes a mistake and uses personal data collected by another controller for a different purpose. The mistake is found before the report is created, and nobody has access to personal data he or she should not have had access to.

How should the processor act on this situation and what should the controller do, if anything?

- A. The processor must notify the controller and the controller must notify the Data Protection Authority of a data breach.
- B. The processor must notify the controller of a data breach. The controller must assess the possible risk to the data subjects.
- C. The processor must notify the Data Protection Authority of a data breach. The controller must execute a PIA to assess the risk to data subjects.
- D. The processor must restart processing using the right data. There is no need for the controller to act.

Answer: B

3.The Supervisory Authority is notified whenever an organization intends to process personal data, except for some specific situations. The Supervisory Authority keeps a publicly accessible register of these data processing operations.

What else is a legal obligation of the Supervisory Authority in reaction to such a notification?

- A. To assess compliance with the law in all classes where sensitive personal data is processed
- B. To assess the legitimacy of operations that involve specific risks for the data subjects
- C. To assess the legitimacy of binding contract(s) between the controller and the data processor(s)
- D. To give out a license for the data processing, specifying the types of personal data which are allowed

Answer: A

4.In what way are online activities of people most effectively used by modern marketers?

- A. By analyzing the logs of the web server it can be seen which products are top sellers, allowing them to optimize their marketing campaigns for those products.
- B. By tagging users of social media, profiles of their online behavior can be created. These profiles are used to ask them to promote a product.
- C. By tagging visitors of web pages, profiles of their online behavior can be created. These profiles are sold and used in targeted advertisement campaigns.

Answer: A

5. A German company wants to enter into a binding contract with a processor in the Netherlands for the processing of sensitive personal data of German data subjects. The Dutch Supervisory Authority is informed of the type of data and the aims of the processing, including the contract describing what data will be processed and what data protection procedures and practices will be in place.

According to the GDPR, what should the Dutch Supervisory Authority do in this scenario?

- A. Report the data processing to the German Supervisory Authority and leave the supervising to them.
- B. Supervise the processing of personal data in accordance with Dutch Law.
- C. Supervise the processing of personal data in accordance with German Law.
- D. The Dutch Supervisory Authority should check that adequate binding contracts are in place. The German Supervisory Authority should supervise.

Answer: D