Vendor:EXIN

Exam Code:PDPF

Exam Name: Privacy and Data Protection Foundation

Version: Demo

QUESTION 1

Personal data as defined in the GDPR can be divided into several types. One of these types is described: Data that directly or indirectly reveal someone\\'s racial or ethnic background, political, philosophical, religious views, union affiliation and data related to health or sex life and sexual orientation. What type of personal data is this?

A. Direct personal data

B. Indirect personal data

C. Pseudonymized data

D. Special category personal data

Correct Answer: D

Direct personal data. Incorrect. Both direct and indirect data are described.

Indirect personal data. Incorrect. Both direct and indirect data are described.

Pseudonymized data. Incorrect. Pseudonymized data cannot directly reveal information.

Special category personal data. Correct. This is a definition of special category personal data. (Literature:

A, Chapter 1; GDPR Article 4)

QUESTION 2

Which of the following options is provided for in the GDPR and can be made by Member States?

A. Approve national provisions for implementation of GDPR.

B. Forcing the controller to notify the data subject of a breach.

C. Audit controller and processor safety processes.

D. Penalize controllers and processors.

Correct Answer: A

Recital 10 of GDPR states:

"Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation."

It also says: "This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data (`sensitive data\\').

However, this does not mean that Member States can approve a rule that goes against a GDPR guideline. Note that these national provisions are measures to increase the effectiveness of the law. Here is an example the case of Ireland where it was established that the DPO is responsible for data breaches, something that is not provided for in the GDPR.

QUESTION 3

A personal data breach has occurred, and the controller is writing a draft notification for the supervisory authority. The following information is already in the notification:

-The nature of the personal data breach and its possible consequences.

-Information regarding the parties that can provide additional information about the data breach.

What other information must the controller provide?

A. Information of local and national authorities that were informed about the data breach.

B. Name and contact details of the data subjects whose data may have been breached

C. Suggested measures to mitigate the adverse consequences of the data breach.

D. The information needed to access the personal data that have been breached.

Correct Answer: C

Information of local and national authorities that were informed about the data breach. Incorrect. The supervisory authority must be made aware of reports to supervisory authorities in other EEA countries. Reports to local authorities, for instance the police, do not need to be reported.

Name and contact details of the data subjects whose data may have been breached. Incorrect. The supervisory authority requires an estimate of the number of data subjects involved, not their personal data.

Suggested measures to mitigate the adverse consequences of the data breach. Correct. The controller should add suggested measures to mitigate the adverse consequences of the data breach. (Literature: A, Chapter 7; GDPR Article 33(q))

The information needed to access the personal data that have been breached. Incorrect. The supervisory authority needs to know the type of personal data involved, but does not need access to the data themselves.

QUESTION 4

For processing of personal data to be legal, a number of requirements must be fulfilled.

What is a requirement for lawful personal data processing?

A. A `code of conduct\\', describing what the processing exactly entails, must be in place.

B. The data subject must have given consent, prior to the processing to begin.

C. The processing must be reported to and allowed by the Data Processing Authority

D. There must be a legitimate ground for the processing of personal data.

Correct Answer: D

QUESTION 5

How does a Supervisory Authority collaborate to the application of GDPR?

A. Assists in the implementation of a data protection management system (at controller request).

B. Monitor and enforce the application of this Regulation.

C. Perform a Data Privacy Impact Analysis (DPI) at the request of the Data Protection Officer ?DPO.

D. Determines technical safety measures to be applied to the controller.

Correct Answer: B

Article 57 legislates on the Responsibilities of the Supervisory Authority. In paragraph 1, item "a" says: "monitor and enforce the application of this Regulation".

QUESTION 6

Data protection and privacy are closely related terms. Which of these options best represent this relationship?

A. Privacy is a part of data protection that aims to keep personal data confidential.

B. Data protection is a part of privacy that aims to keep personal data confidential.

C. The two terms have the same meaning. They are synonymous.

D. Without protection of personal data there is no privacy.

Correct Answer: D

A very repeated phrase is: "It is possible to have security without privacy, but it is not possible to have privacy without security".

Privacy is a right that should be protected, and Data Protection are the measures that will be used to achieve this protection.

QUESTION 7

A secretary at a pediatric cardiology clinic instead of sending the doctor the list of patients scheduled for the day, sends it to all those responsible registered for the children with scheduled appointments.

According to the GDPR, does the Supervisory Authority need to be notified? And those responsible for the data holders?

A. The Supervisory Authority must be notified, but there is no need to notify those responsible for the data subjects, as whoever had access to the data is also someone in the same situation.

B. The Supervisory Authority must be notified and also those responsible for the holders who had their data exposed.

C. There is no need to notify the Supervisory Authority, however those responsible for the holders who had their data exposed must be notified.

D. There is no need to notify the Supervisory Authority or those responsible for the data subjects, as whoever had access to the data is also someone in the same situation.

Correct Answer: B

This is an issue that addresses two very important points ?sensitive data and data from minors.

As these are, it is necessary to inform the Supervisory Authority and those responsible for the data subjects.

Article 34 mentions:

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Recital 38 says:

Children merit specific protection regarding their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

QUESTION 8

A breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. What is the exact term that is associated with this definition in the GDPR?

A. Security breach

B. Personal data breach

C. Confidentiality violation

D. Security incident

Correct Answer: B

Confidentiality violation. Incorrect. GDPR uses the term personal data breach. Not every data breach is a confidentiality violation.

Personal data breach. Correct. This is the definition of a personal data breach. (Literature: A, Chapter 5; GDPR Article 4(12))

Security breach. Incorrect. GDPR uses the term personal data breach. Not every security breach is a data breach. Not every data breach is a personal data breach.

Security incident. Incorrect. GDPR uses the term personal data breach. Not every security incident is a data breach.

QUESTION 9

According to the GDPR, what is a mandatory topic in a DPIA report?

A. Systematic description of the fiduciary duties to ensure compliance to all relevant laws and regulations

B. An assessment of the necessity and proportionality of the processing operations in relation to the purposes

C. The documentation of the risks to the rights and freedoms of the data protection officer

D. The measures envisaged to address the privacy compliance frameworks risks

Correct Answer: B

QUESTION 10

Which cause is a data breach according to the GDPR?

A. illegally obtained corporate data from a human resources management system

B. Personal data is processed without a binding contract.

C. Personal data is processed by anyone other than the controller, processor or, possibly, subprocessor

D. The operation of a vulnerable server in the internal network of the processor

Correct Answer: A

QUESTION 11

Who is responsible for demonstrating the compliance of personal data processing with the General Data Protection Regulation (GDPR)?

A. The Data Protection Officer (DPO)

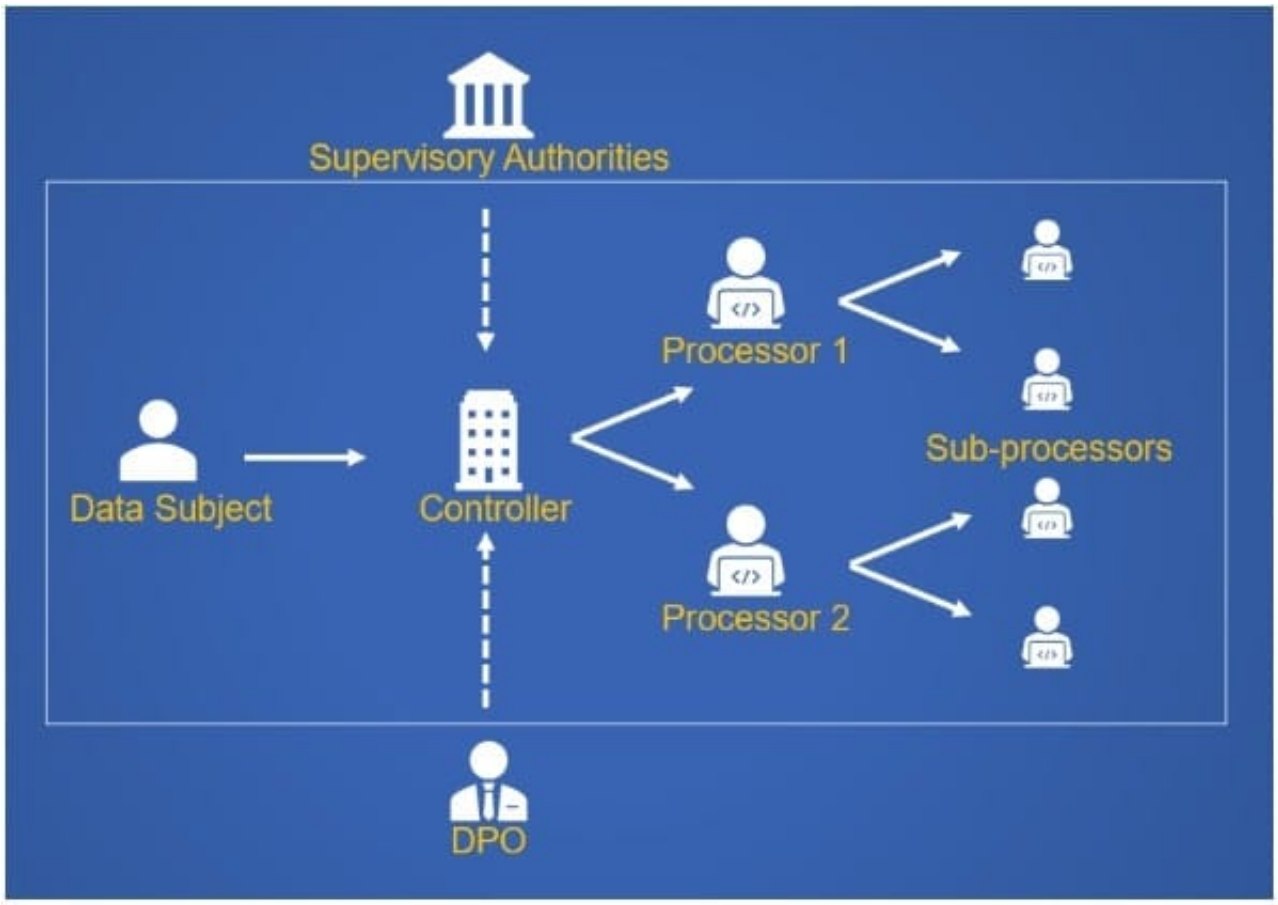
B. The processor

C. The controller

D. The supervisory authority

Correct Answer: C

The front line with the data holder is the Controller, see image. So, it is he who has to show compliance, who must be concerned with the legality of processing, who must implement security measures.



QUESTION 12

To comply with the General Data Protection Regulation (GDPR) it is necessary to create a procedure for reporting data breaches to the Supervisory Authority.

As the controller is a public administration agency, which option is a requirement for this procedure?

A. It must contain a step to perform a Data Protection Impact Analysis (DPIA).

B. It must include an audit step.

C. It should include a step to consult the Data Protection Officer (DPO) in order to determine whether notification to the Supervisory Authority is necessary.

D. It must contain a step to notify the data subject.

Correct Answer: C

It is not necessary to inform the Supervisory Authority of any violation that occurs. But every violation must be analyzed with caution and attention. It is not necessary to notify the Supervisory Authority only if it does not present risks to the data subjects.

The DPO must always be involved to guide the best strategy and action for each violation that occurs.

Article 38 legislates on the position of the data protection officer:

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

It is clear that the DPO ?Data Protection Officer, must be involved in the entire data processing life cycle. From its collection to its exclusion.