PDPF Q&As

Privacy and Data Protection Foundation

Pass EXIN PDPF Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/pdpf.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EXIN Official Exam Center

QUESTION 1

In the European Union we have: Directives and Regulations. What is the difference between them?

A. The regulation provides guidance for EU Member States and they can create their own laws to conform to the regulation. A directive has the force of law and all EU Member States must follow it without changing it.

B. The directive provides guidance for EU member states and they can create their own laws to suit the directive. A regulation has the force of law and all EU Member States must follow it without changing it.

Correct Answer: B

When we have a Regulation, such as the GDPR, all EU member states are obliged to follow it and have a fixed date for entry into force. The regulation is a law and Member States cannot create laws that oppose it. Unlike the Directives that set objectives to be achieved, however, each Member State is free to decide how to apply them in its country.

Important

Prior to the GDPR, there was the "95/46 / EC First Data Protection Directive (European DP)". Approved in 1995, it was already aimed to protect personal data. This directive was replaced by the GDPR.

"Article 94: 1. Directive 95/46 / EC is repealed with effect from 25 May 2018."

In the EXIN PDPF exam this is a question that is routinely asked. "What directive has been replaced by GDPR?" Answer: 95/46 / EC.

QUESTION 2

An architect, leaving a building site, puts his laptop for a moment beside his car on the road, while answering his phone. When driving away he sees in the mirror his laptop being crushed by an enormous lorry driving over it. All his files on the design of the building and the calculations he worked on are lost. His only consolation is that those were the only files on the device.

In terms of the GDPR, what happened?

A. a data breach

B. a security incident

C. a security issue

D. a vulnerability

Correct Answer: B

QUESTION 3

Which organizations need to comply with the General Data Protection Regulation (GDPR)?

A. Only organizations that have employees in the European Union (EU).

B. Only organizations that have their headquarters in the European Union (EU).

C. All organizations anywhere in the world.

D. All organizations located in the European Union and also organizations outside the European Union that offer goods or services to data subjects in the EU.

Correct Answer: D

This is a question that has the most doubts: "Who needs to adapt?". For example: 1 - If you have a company in Brazil and sell products or services and process personal data from residents in the EU, in this case your company must conform to the GDPR. 2- If you have a company located in the EU and handle personal data.

Transcribing here part of Article 3 of the GDPR:

1.

This Regulation applies to the processing of personal data carried out in the context of the activities of an establishment of a controller or a subcontractor located in the territory of the Union, regardless of whether the processing takes place inside or outside the Union.

2.

This Regulation applies to the processing of personal data of holders residing in the territory of the Union, carried out by a controller or processor not established in the Union, when the processing activities are related to:

a) The provision of goods or services to such data subjects in the Union, regardless of the requirement for data subjects to make a payment;

b) Control of their behavior, provided that such behavior takes place in the Union.

QUESTION 4

A controller can contract out the processing of personal data to another company, provided a written contract between these partners is in place.

Which clause in this contract is a responsibility of the controller?

A. To ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

B. To make available all information necessary to demonstrate compliance with the obligations laid down in the GDPR and allow for and contribute to audits, including inspections.

C. To process the personal data only on documented instructions, including with regard to transfers of personal data to a third country or an international organization.

D. To provide sufficient guarantees for appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR.

Correct Answer: A

QUESTION 5

According to the GDPR, what is a description of binding corporate rules (BCR)?

A. A decision on the safety of transferring personal data to a non-EEA country

B. A set of approved rules on personal data protection used by a group of enterprises

C. A measure to compensate for the lack of personal data protection in a third country

D. A set of agreements covering personal data transfers between non-EEA countries

Correct Answer: B

A decision on the safety of transferring personal data to a non-EEA country. Incorrect. This refers to adequacy decisions.

A measure to compensate for the lack of personal data protection in a third country. Incorrect. This refers to appropriate safeguards.

A set of agreements covering personal data transfers between non-EEA countries. Incorrect. The GDPR does not cover agreements between non-EEA countries.

A set of approved rules on personal data protection used by a group of enterprises. Correct. BCR are a set of rules approved by the supervisory authorities. (Literature: A, Chapter 3; GDPR Article 47)

QUESTION 6

According to Article.33 of the GDPR the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.

What is the maximum penalty for non-compliance with this notification obligation?

A. 10.000.000 or 2% of the annual global turnover, whichever is higher

B. 20.000.000 or 4% of the annual global turnover, whichever is higher

C. Up to 500.000 with a minimum of 120.000

D. Up to 820.000 with a minimum of 350.000

Correct Answer: A

10.000.000 or 2% of the annual global turnover, whichever is higher. Correct. This is the maximum according to the GDPR for infringement of the personal data breach notification obligation. (Literature: A, Chapter 7; GDPR Article 33)

20.000.000 or 4% of the annual global turnover, whichever is higher. Incorrect. This fine is given for noncompliance or non-conformity to the basic principles for processing, including conditions for consent. Up to

500.000 with a minimum of 120.000. Incorrect. This is an outdated number based on the Dutch Penal code. GDPR rules specify higher fines.

Up to 820.000 with a minimum of 350.000. Incorrect. This is an outdated number based on the Dutch Penal code. GDPR rules specify higher fines.

QUESTION 7

One of the basic principles of the General Data Protection Regulation (GDPR) is subsidiarity.

What is subsidiarity to GDPR?

A. Personal data can only be collected for explicit, legitimate and specific purposes and cannot be processed for any other purpose.

B. Only the personal data needed to achieve a specific purpose should be collected.

C. The least privacy-violating means should be used when processing personal data.

D. Personal data must be kept for a period not longer than necessary.

Correct Answer: C

Whereas Recital 170 mentions: "Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective".

Subsidiarity is a principle that says that personal data can only be processed if there are no other means to achieve the objective. Therefore, the less personal data used, the less the chances of violating privacy.

Note that in the quotation in Recital 170 above, the principle of proportionality was highlighted in bold.

Equally important to subsidiarity. Proportionality says that personal data must be collected according to the purpose of processing, that is proportional, and data that will not be used for the purpose should not be collected.

These two principles Subsidiarity and Proportionality are constantly charged in the EXIN exam.

QUESTION 8

We know that when a personal data breach occurs, the data controller (Controller) must notify the Supervisory Authority within 72 hours, without justified delay. However, should the Controller do if it is unable to communicate within this time?

A. Send the notification with the date of the violation changed, to remain within 72 hours.

B. After 72 hours there is no longer any need to send notification of personal data breach.

C. Do not notify and seek ways to hide the violation so that the Supervisory Authority or the titleholders are made aware

D. Send the notification, even after 72 hours, accompanied by the reasons for the delay

Correct Answer: D

Article 33 which deals with "Notification of a personal data breach to the supervisory authority" in its paragraph 1 legislates:

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

QUESTION 9

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 10

According to the GDPR, what is a task of a supervisory authority?

A. Investigate security breaches of corporate information

B. Implement technical and organizational measures to ensure compliance

C. Monitor and enforce the application of the GDPR

Correct Answer: C

Implement technical and organizational measures to ensure compliance. Incorrect. This is the task of the controller.

Investigate security breaches of corporate information. Incorrect. Only breaches of personal data are a concern of the supervisory authority.

Monitor and enforce the application of the GDPR. Correct. This is the main task of any supervisory authority. (Literature: A, Chapter 7)

QUESTION 11

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.

Correct Answer: A

QUESTION 12

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

A. The Data Protection Officer (DPO)

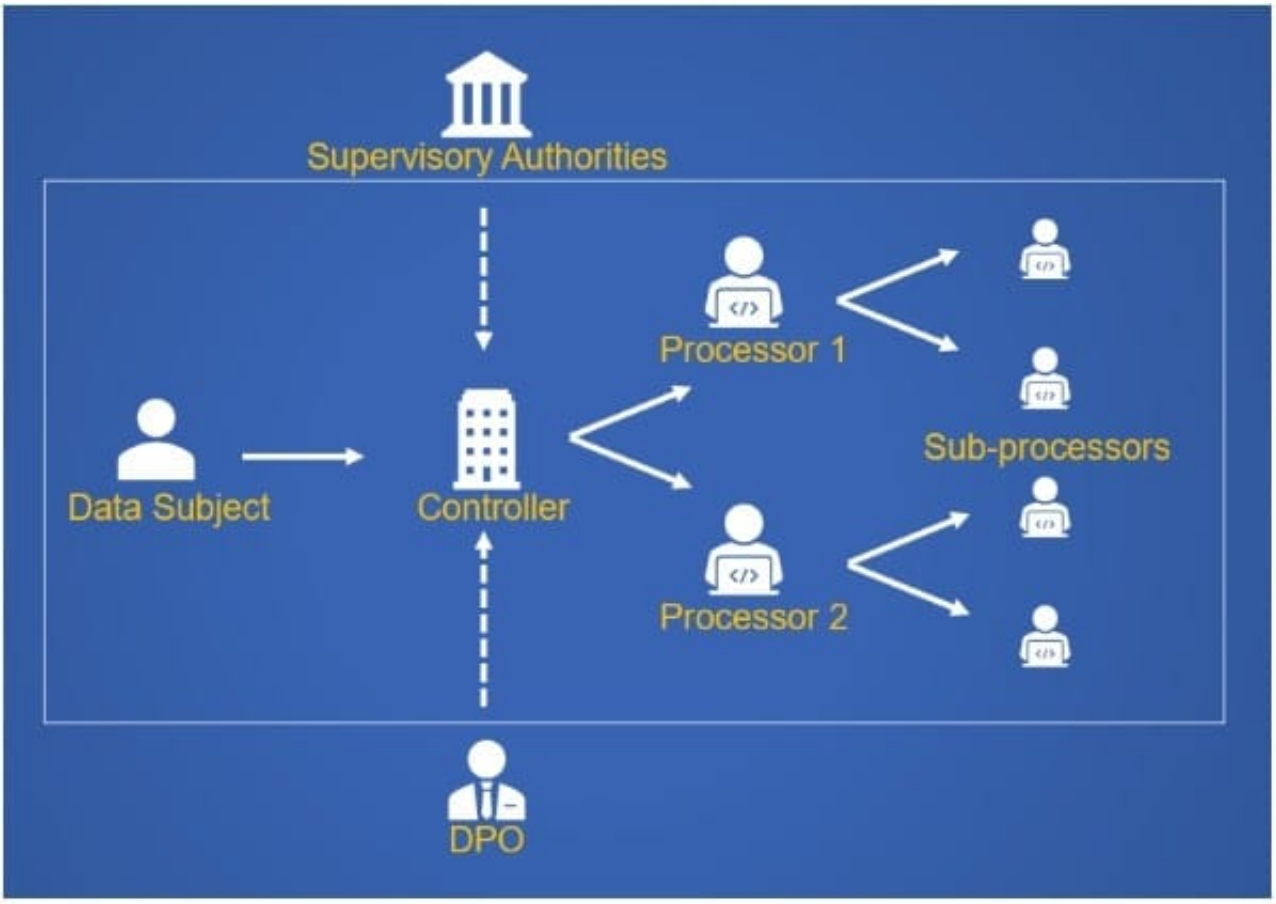
B. The processor

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 13

Personal data can be transferred outside of the EEA. According to the GDPR, which transfers outside the EEA are always lawful?

A. Transfers based on the laws of the non-EEA country concerns

B. Transfers falling under World Trade Organization rules

C. Transfers governed by approved binding corporate rules (BCR)

D. Transfers within a global corporation or organization

Correct Answer: C

Transfers based on the laws of the non-EEA country concerned. Incorrect. This would also require an adequacy decision confirming that those laws are sufficient.

Transfers falling under World Trade Organization rules. Incorrect. WTO only covers free trade of goods and services.

Transfers governed by approved binding corporate rules (BCR). Correct. Binding corporate rules approved by a supervisory authority involved make the transfer lawful. (Literature: A, Chapter 7; GDPR Article 47)

Transfers within a global corporation or organization. Incorrect. This would also require that they adopt official binding corporate rules.

Reference: https://edps.europa.eu/data-protection/data-protection/reference-library/internationaltransfers_en

QUESTION 14

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 15

What is the legal status of the GDPR?

A. The GDPR is functional law in all member states of the EEA. Some Articles allow for member states law to provide for more specific rules.

B. The GDPR sets out minimum conditions and requirements. Member states need to pass national laws to meet these minimum requirements.

C. The GDPR is a recommendation of the European Commission that EEA countries\\' law authorities improve their laws on the protection of personal data.

Correct Answer: A

The GDPR is functional law in all member states of the EEA. Some Articles allow for member states law to provide for more specific rules. Correct. The GDPR is European law but the Regulation does not exclude Member state law that sets out the circumstances for specific processing situations. (Literature: A, Chapter 1; GDPR Recital 10)

The GDPR is a recommendation of the European Commission that EEA countries\\' law authorities improve their laws on the protection of personal data. Incorrect. An EU recommendation is not binding. The GDPR is a functional European law in all member states.

The GDPR sets out minimum conditions and requirements. Member states need to pass national laws to meet these minimum requirements. Incorrect. This is the description of an EU Directive.