

GDPR考古題介紹 - GDPR學習指南



2025 PDFExamDumps最新的GDPR PDF版考試題庫和GDPR考試問題和答案免費分享：<https://drive.google.com/open?id=1S834HoFSEncbkUaipruMPf4eyQ-X9r0G>

您可以先在網上免費下載PDFExamDumps提供的部分關於PECB GDPR 認證考試的練習題和答案來測試我們的品質。PDFExamDumps能夠幫你100%通過PECB GDPR 認證考試，如果你不小心沒有通過PECB GDPR 認證考試，我們保證會全額退款。

PECB GDPR 考試大綱：

主題	簡介
主題 1	<ul style="list-style-type: none">Technical and organizational measures for data protection: This section of the exam measures the skills of IT Security Specialists and covers the implementation of technical and organizational safeguards to protect personal data. It evaluates the ability to apply encryption, pseudonymization, and access controls, as well as the establishment of security policies, risk assessments, and incident response plans to enhance data protection and mitigate risks.
主題 2	<ul style="list-style-type: none">Data protection concepts: General Data Protection Regulation (GDPR), and compliance measures
主題 3	<ul style="list-style-type: none">Roles and responsibilities of accountable parties for GDPR compliance: This section of the exam measures the skills of Compliance Managers and covers the responsibilities of various stakeholders, such as data controllers, data processors, and supervisory authorities, in ensuring GDPR compliance. It assesses knowledge of accountability frameworks, documentation requirements, and reporting obligations necessary to maintain compliance with regulatory standards.
主題 4	<ul style="list-style-type: none">This section of the exam measures the skills of Data Protection Officers and covers fundamental concepts of data protection, key principles of GDPR, and the legal framework governing data privacy. It evaluates the understanding of compliance measures required to meet regulatory standards, including data processing principles, consent management, and individuals' rights under GDPR.

GDPR學習指南 - GDPR認證考試解析

PDFExamDumps擁有龐大的IT專家團隊，他們不斷利用自己的知識和經驗研究很多過去幾年的IT認證考試試題。他們的研究成果即是我們的PDFExamDumps的產品，因此PDFExamDumps提供的PECB GDPR練習題和真實的考試練習題有很大的相似性，可以幫助很多人實現他們的夢想。PDFExamDumps可以確保你成功通過考試，你是可以大膽地將PDFExamDumps加入你的購物車。有了PDFExamDumps你的夢想馬上就可以實現了。

最新的 Privacy And Data Protection GDPR 免費考試真題 (Q33-Q38):

問題 #33

Scenario5:

Repond is a German employment recruiting company. Their services are delivered globally and include consulting and staffing solutions. In the beginning, Repond provided its services through an office in Germany. Today, they have grown to become one of the largest recruiting agencies, providing employment to more than 500,000 people around the world. Repond receives most applications through its website. Job searchers are required to provide the job title and location. Then, a list of job opportunities is provided. When a job position is selected, candidates are required to provide their contact details and professional work experience records. During the process, they are informed that the information will be used only for the purposes and period determined by Repond. Repond's experts analyze candidates' profiles and applications and choose the candidates that are suitable for the job position. The list of the selected candidates is then delivered to Repond's clients, who proceed with the recruitment process. Files of candidates that are not selected are stored in Repond's databases, including the personal data of candidates who withdraw the consent on which the processing was based. When the GDPR came into force, the company was unprepared.

The top management appointed a DPO and consulted him for all data protection issues. The DPO, on the other hand, reported the progress of all data protection activities to the top management. Considering the level of sensitivity of the personal data processed by Repond, the DPO did not have direct access to the personal data of all clients, unless the top management deemed it necessary. The DPO planned the GDPR implementation by initially analyzing the applicable GDPR requirements. Repond, on the other hand, initiated a risk assessment to understand the risks associated with processing operations. The risk assessment was conducted based on common risks that employment recruiting companies face. After analyzing different risk scenarios, the level of risk was determined and evaluated. The results were presented to the DPO, who then decided to analyze only the risks that have a greater impact on the company. The DPO concluded that the cost required for treating most of the identified risks was higher than simply accepting them. Based on this analysis, the DPO decided to accept the actual level of the identified risks. After reviewing policies and procedures of the company, Repond established a new data protection policy. As proposed by the DPO, the information security policy was also updated. These changes were then communicated to all employees of Repond. Based on this scenario, answer the following question:

Question:

According to scenario 5, what should Repond have considered when assessing the risks related to processing operations?

- A. Risks should be assessed only when a supervisory authority requires it.
- B. Risks should be assessed based on the risk-based approach adopted by the DPO.
- C. Risks should be analyzed using a quantitative approach, since risk scenarios make the evaluation process difficult.
- **D. Risks should be identified based on threats and vulnerabilities that the company faces.**

答案: D

解題說明:

Under Article 32 of GDPR, risk assessments should be based on threats, vulnerabilities, and potential impact on data subjects. Organizations must identify and mitigate risks to personal data security.

* Option A is correct because risk identification should consider threats, vulnerabilities, and impact.

* Option B is incorrect because risk can be assessed qualitatively or quantitatively, depending on the approach used.

* Option C is incorrect because DPOs do not define an organization's risk-based approach.

* Option D is incorrect because risk assessment is mandatory under GDPR, not only when a supervisory authority requests it.

References:

* GDPR Article 32(1)(Risk-based approach to security)

* Recital 83(Risk assessment in data protection)

問題 #34

Scenario4:

Berc is a pharmaceutical company headquartered in Paris, France, known for developing inexpensive improved healthcare products. They want to expand to developing life-saving treatments. Berc has been engaged in many medical researches and clinical trials over the years. These projects required the processing of large amounts of data, including personal information. Since 2019, Berc has pursued GDPR compliance to regulate data processing activities and ensure data protection. Berc aims to positively impact human health through the use of technology and the power of collaboration. They recently have created an innovative solution in participation with Unty, a pharmaceutical company located in Switzerland. They want to enable patients to identify signs of strokes or other health-related issues themselves. They wanted to create a medical wrist device that continuously monitors patients' heart rate and notifies them about irregular heartbeats. The first step of the project was to collect information from individuals aged between 50 and 65. The purpose and means of processing were determined by both companies. The information collected included age, sex, ethnicity, medical history, and current medical status. Other information included names, dates of birth, and contact details. However, the individuals, who were mostly Berc's and Unty's customers, were not aware that there was an arrangement between Berc and Unty and that both companies have access to their personal data and share it between them. Berc outsourced the marketing of their new product to an international marketing company located in a country that had not adopted the adequacy decision from the EU commission. However, since they offered a good marketing campaign, following the DPO's advice, Berc contracted it. The marketing campaign included advertisement through telephone, emails, and social media. Berc requested that Berc's and Unty's clients be first informed about the product. They shared the contact details of clients with the marketing company. Based on this scenario, answer the following question:

Question:

Based on scenario 4, Berc followed the DPO's advice for outsourcing an international marketing company in the absence of an adequacy decision. Is the DPO responsible for evaluating this case?

- A. Yes, the DPO should evaluate cases where an adequacy decision is absent.
- B. No, because the marketing company operates under the same data protection rules as Berc.
- **C. No, the controller or processor should evaluate cases when the adequacy decision is absent.**
- D. Yes, the DPO takes the final decision on transferring personal data to an international company in the absence of an adequacy decision.

答案: C

解題說明:

Under Article 44 of GDPR, the controller (Berc) is responsible for ensuring lawful data transfers. The DPO advises on compliance but does not make final decisions on data transfers.

- * Option C is correct because the controller (Berc) must evaluate the legality of the transfer.
- * Option A is incorrect because DPOs provide advice but do not evaluate data transfer legality.
- * Option B is incorrect because DPOs do not have executive decision-making authority.
- * Option D is incorrect because data protection rules vary by jurisdiction, making this assumption incorrect.

References:

- * GDPR Article 44 (General principle for transfers)
- * GDPR Article 39(1)(a) (DPO's advisory role)

問題 #35

Scenario 6:

Bus Spot is one of the largest bus operators in Spain. The company operates in local transport and bus rental since 2009. The success of Bus Spot can be attributed to the digitization of the bus ticketing system, through which clients can easily book tickets and stay up to date on any changes to their arrival or departure time. In recent years, due to the large number of passengers transported daily, Bus Spot has dealt with different incidents including vandalism, assaults on staff, and fraudulent injury claims. Considering the severity of these incidents, the need for having strong security measures had become crucial. Last month, the company decided to install a CCTV system across its network of buses. This security measure was taken to monitor the behavior of the company's employees and passengers, enabling crime prevention and ensuring safety and security. Following this decision, Bus Spot initiated a data protection impact assessment (DPIA). The outcome of each step of the DPIA was documented as follows:

Step 1: In all 150 buses, two CCTV cameras will be installed. Only individuals authorized by Bus Spot will have access to the information generated by the CCTV system. CCTV cameras capture images only when the Bus Spot's buses are being used. The CCTV cameras will record images and sound. The information is transmitted to a video recorder and stored for 20 days. In case of incidents, CCTV recordings may be stored for more than 40 days and disclosed to a law enforcement body. Data collected through the CCTV system will be processed by another organization. The purpose of processing this type of information is to increase the security and safety of individuals and prevent criminal activity.

Step 2: All employees of Bus Spot were informed for the installation of a CCTV system. As the data controller, Bus Spot will have the ultimate responsibility to conduct the DPIA. Appointing a DPO at that point was deemed unnecessary. However, the data processor's suggestions regarding the CCTV installation were taken into account.

Step 3: Risk Likelihood (Unlikely, Possible, Likely) Severity (Moderate, Severe, Critical) Overall risk (Low, Medium, High) There is a risk that the principle of lawfulness, fairness, and transparency will be compromised since individuals might not be

aware of the CCTV location and its field of view. Likely Moderate Low There is a risk that the principle of integrity and confidentiality may be compromised in case the CCTV system is not monitored and controlled with adequate security measures. Possible Severe Medium There is a risk related to the right of individuals to be informed regarding the installation of CCTV cameras. Possible Moderate Low Step 4: Bus Spot will provide appropriate training to individuals that have access to the information generated by the CCTV system. In addition, it will ensure that the employees of the data processor are trained as well. In each entrance of the bus, a sign for the use of CCTV will be displayed. The sign will be visible and readable by all passengers. It will show other details such as the purpose of its use, the identity of Bus Spot, and its contact number in case there are any queries. Only two employees of Bus Spot will be authorized to access the CCTV system. They will continuously monitor it and report any unusual behavior of bus drivers or passengers to Bus Spot. The requests of individuals that are subject to a criminal activity for accessing the CCTV images will be evaluated only for a limited period of time. If the access is allowed, the CCTV images will be exported by the CCTV system to an appropriate file format. Bus Spot will use a file encryption software to encrypt data before transferring onto another file format. Step 5: Bus Spot's top management has evaluated the DPIA results for the processing of data through CCTV system. The actions suggested to address the identified risks have been approved and will be implemented based on best practices. This DPIA involves the analysis of the risks and impacts in only a group of buses located in the capital of Spain. Therefore, the DPIA will be reconducted for each of Bus Spot's buses in Spain before installing the CCTV system. Based on this scenario, answer the following question:

Question:

Which step of the DPIA methodology did Bus Spot miss when conducting the DPIA?

- A. The supervisory authority approval step, where it should have obtained prior authorization before implementing the CCTV system.
- **B. The necessity and proportionality evaluation step, where it should have determined the lawful basis for data processing.**
- C. The step describing the data processing activities, where it should have detailed the scope, nature, context, and purposes of the processing.
- D. The alignment with GDPR-defined DPIA guidelines, where it should have adhered to the regulatory framework and methodology outlined by the GDPR.

答案： B

解題說明：

Under Article 35(7)(b) of GDPR, a DPIA must include an assessment of the necessity and proportionality of processing. This ensures that data processing is lawful, limited, and justified. Bus Spot missed this step, which is essential for verifying the lawful basis for processing CCTV data.

* Option A is correct because the necessity and proportionality assessment was required but not completed.

* Option B is incorrect because Bus Spot documented data processing activities in the DPIA.

* Option C is incorrect because not aligning with GDPR guidelines does not automatically invalidate a DPIA.

* Option D is incorrect because prior approval from a supervisory authority is only required if high-risk processing is detected without sufficient mitigation measures (Article 36).

References:

* GDPR Article 35(7)(b) (Necessity and proportionality in DPIAs)

* Recital 90 (Assessing necessity in a DPIA)

問題 #36

Scenario 4:

Berc is a pharmaceutical company headquartered in Paris, France, known for developing inexpensive improved healthcare products. They want to expand to developing life-saving treatments. Berc has been engaged in many medical researches and clinical trials over the years. These projects required the processing of large amounts of data, including personal information. Since 2019, Berc has pursued GDPR compliance to regulate data processing activities and ensure data protection. Berc aims to positively impact human health through the use of technology and the power of collaboration. They recently have created an innovative solution in participation with Unty, a pharmaceutical company located in Switzerland. They want to enable patients to identify signs of strokes or other health-related issues themselves. They wanted to create a medical wrist device that continuously monitors patients' heart rate and notifies them about irregular heartbeats. The first step of the project was to collect information from individuals aged between 50 and 65. The purpose and means of processing were determined by both companies. The information collected included age, sex, ethnicity, medical history, and current medical status. Other information included names, dates of birth, and contact details. However, the individuals, who were mostly Berc's and Unty's customers, were not aware that there was an arrangement between Berc and Unty and that both companies have access to their personal data and share it between them. Berc outsourced the marketing of their new product to an international marketing company located in a country that had not adopted the adequacy decision from the EU commission. However, since they offered a good marketing campaign, following the DPO's advice, Berc contracted it. The marketing campaign included advertisement through telephone, emails, and social media. Berc requested that Berc's and Unty's clients be first informed about the product. They shared the contact details of clients with the marketing

company. Based on this scenario, answer the following question:

Question:

Is the transfer of data from Berc to Unty in compliance with GDPR?

- A. No, Berc must conduct a new DPIA before transferring data to Switzerland.
- B. No, Berc cannot transfer data to a company in Switzerland unless authorization from the supervisory authority in France is obtained.
- C. Yes, Berc can transfer data to Unty because they collected data for the same purpose.
- **D. Yes, Berc can transfer data to Unty because Switzerland provides a level of data protection that is "essentially equivalent" to that of the EU.**

答案: D

解題說明:

Under Article 45 of GDPR, data transfers to third countries are lawful if the European Commission has adopted an adequacy decision, meaning the country offers equivalent protection to GDPR. Switzerland has such an adequacy decision, making Berc's transfer lawful.

* Option A is correct because Switzerland meets GDPR adequacy standards.

* Option B is incorrect because having the same purpose does not automatically make the transfer lawful.

* Option C is incorrect because no supervisory authorization is needed when an adequacy decision exists.

* Option D is incorrect because a DPIA is not required for a GDPR-compliant transfer.

References:

* GDPR Article 45(1)(Adequacy decisions for third countries)

* European Commission Decision on Switzerland's adequacy

問題 #37

Scenario:

An organization has been using a storage transfer service to import market-sensitive data, including email addresses and contact details, into a cloud storage system. This change has affected the registration process and has helped the organization appropriately collect and store data.

Question:

Based on this scenario, what should the DPO monitor in the data processing register?

- **A. Whether the changes have been reflected in the data processing registers.**
- B. Whether the organization has obtained consent from the data subjects for this change.
- C. Whether the organization has notified the supervisory authority about the change in storage methods.
- D. Whether the organization has identified storage transfer service's technical and organizational measures for protection of personal data.

答案: A

解題說明:

Under Article 30 of GDPR, controllers and processors must maintain a record of processing activities (ROPA). Whenever changes occur in the way personal data is processed (such as a transfer to cloud storage), the DPO must ensure these changes are recorded in the processing register.

* Option B is correct because the DPO must ensure the data processing register is updated to reflect the new storage method.

* Option A is incorrect because storage changes do not require new consent unless the purpose of processing has changed.

* Option C is incorrect because while assessing security measures is important, it is not the primary duty related to the data processing register.

* Option D is incorrect because not all processing changes require notifying the supervisory authority unless they introduce high risks without proper safeguards.

References:

* GDPR Article 30(1)(g)(Controllers must maintain updated processing records)

* Recital 82(Controllers should document changes in processing activities)

問題 #38

.....

我們 PDFExamDumps PECB 的 GDPR 考試的做法是最徹底的，以及最準確及時的最新的實踐檢驗，你會發現目前市場上的唯一可以有讓你第一次嘗試通過困難的信心。PECB 的 GDPR 考試認證在世界上任何一個國家將會得到承

GDPR學習指南：https://www.pdfexamdumps.com/GDPR_valid-braindumps.html

- 從Google Drive中免費下載最新的PDFExamDumps GDPR PDF版考試題庫: <https://drive.google.com/open?id=1S834HoFSEncbkUaipruMPf4eyQ-X9r0G>