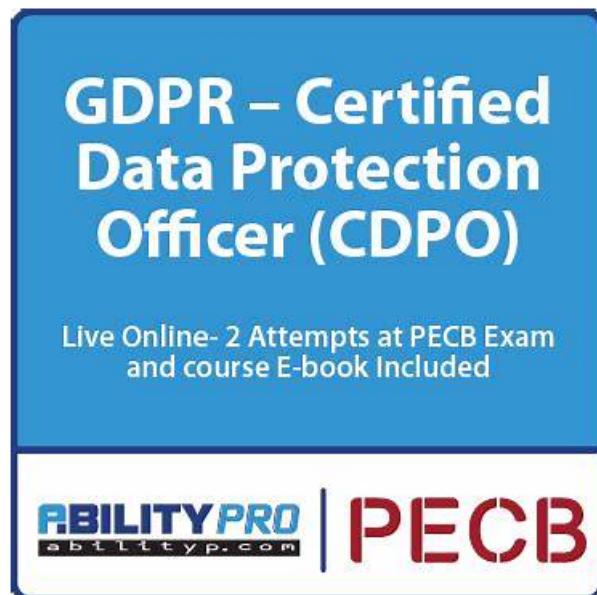


TOP Pdf GDPR Exam Dump - PECB PECB Certified Data Protection Officer - Trustable GDPR Reliable Test Labs



DOWNLOAD the newest PDFVCE GDPR PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1Ohf-KIzEGhX3kKpDgFenq6taKUsinyg>

The committed team of the PDFVCE is always striving hard to resolve any confusion among its users. The similarity between our PECB GDPR exam questions and the real PECB GDPR certification exam will amaze you. The similarity between the PDFVCE GDPR pdf questions and the actual GDPR certification exam will help you succeed in obtaining the highly desired PECB Certified Data Protection Officer (GDPR) certification on the first go. You will notice the above features in the PECB GDPR Web-based format too. There is no need to go through time-taking installations or agitating plugins to use this format.

Our website always trying to bring great convenience to our candidates who are going to attend the GDPR practice test. You can practice our GDPR dumps demo in any electronic equipment with our online test engine. To all customers who bought our GDPR Pdf Torrent, all can enjoy one-year free update. We will send you the latest version immediately once we have any updating about this test.

>> Pdf GDPR Exam Dump <<

PECB GDPR Reliable Test Labs | Valid GDPR Exam Online

The PECB Certified Data Protection Officer PDF practice material contains actual PECB GDPR Exam Questions compiled by certified experts around the globe to benefit candidates. The criteria and pattern of the PECB Certified Data Protection Officer exam often change, and hence it is essential to use the updated exam study material for preparation. PDFVCE provides free updates after purchase so that you get the latest PECB Exam Questions for the exam.

PECB Certified Data Protection Officer Sample Questions (Q39-Q44):

NEW QUESTION # 39

Question:

A patient gave consent for the use of their laboratory tests to defend a clinical laboratory against a lawsuit. As a result, the court required the collection and processing of the patient's health data, and such information was revealed in court. Is this compliant with GDPR's lawfulness of processing requirements?

- A. No, although the data subject has consented to the processing of health data, GDPR does not allow the disclosure of special categories of personal data by health institutions.
- B. No, because personal data used in legal proceedings must be anonymized before being disclosed.
- C. Yes, but only if the processing of special categories of personal data is controlled by a public health institution, and the data subject has consented to the processing of this type of data.
- D. Yes, because the data subject has consented to the processing of health data, and GDPR allows the processing of special categories of data where it is necessary for the establishment, exercise, or defense of legal claims.

Answer: D

Explanation:

Under Article 9(2)(f) of GDPR, the processing of special categories of data (e.g., health data) is permitted without consent if it is necessary for the establishment, exercise, or defense of legal claims.

- * Option A is correct because GDPR allows processing of special category data for legal claims, even without explicit consent.
- * Option B is incorrect because processing for legal claims is not restricted to public health institutions.

- * Option C is incorrect because GDPR explicitly allows such processing for legal claims.

- * Option D is incorrect because anonymization is not required when data is processed under Article 9(2) (f).

References:

* GDPR Article 9(2)(f) (Processing of special categories of data for legal claims)

* Recital 52 (Legal grounds for processing sensitive data in court cases)

NEW QUESTION # 40

Scenario 9: Soin is a French travel agency with the largest network of professional travel agents throughout Europe. They aim to create unique vacations for clients regardless of the destinations they seek. The company specializes in helping people find plane tickets, reservations at hotels, cruises, and other activities.

As any other industry, travel is no exception when it comes to GDPR compliance. Soin was directly affected by the enforcement of GDPR since its main activities require the collection and processing of customers' data.

Data collected by Soin includes customer's ID or passport details, financial and payment information, and contact information. This type of data is defined as personal by the GDPR; hence, Soin's data processing activities are built based on customer's consent.

At the beginning, as for many other companies, GDPR compliance was a complicated issue for Soin.

However, the process was completed within a few months and later on the company appointed a DPO. Last year, the supervisory authority of France, requested the conduct of a data protection external audit in Soin without an early notice. To ensure GDPR compliance before an external audit was conducted, Soin organized an internal audit. The data protection internal audit was conducted by the DPO of the company. The audit was initiated by firstly confirming the accuracy of records related to all current Soin's data processing activities.

The DPO considered that verifying compliance to Article 30 of GDPR would help in defining the data protection internal audit scope. The DPO noticed that not all processing activities of Soin were documented as required by the GDPR. For example, processing activities records of the company did not include a description of transfers of personal data to third countries. In addition, there was no clear description of categories of personal data processed by the company. Other areas that were audited included content of data protection policy, data retention guidelines, how sensitive data is stored, and security policies and practices.

The DPO conducted interviews with some employees at different levels of the company. During the audit, the DPO came across some emails sent by Soin's clients claiming that they do not have access to their personal data stored by Soin. Soin's Customer Service Department answered the emails saying that, based on Soin's policies, a client cannot have access to personal data stored by the company. Based on the information gathered, the DPO concluded that there was a lack of employee awareness on the GDPR.

All these findings were documented in the audit report. Once the audit was completed, the DPO drafted action plans to resolve the nonconformities found. Firstly, the DPO created a new procedure which could ensure the right of access to clients. All employees were provided with GDPR compliance awareness sessions.

Moreover, the DPO established a document which described the transfer of personal data to third countries and the applicability of safeguards when this transfer is done to an international organization.

Based on this scenario, answer the following question:

According to scenario 9, the DPO drafted and implemented all action plans to resolve the nonconformities found. Is this acceptable?

- A. No, the DPO should implement action plans as arranged in order of priority by top management
- B. No, the DPO should only evaluate and follow up on action plans submitted in response to nonconformities

- C. Yes, the DPO is responsible for drafting, implementing, and reviewing corrections and corrective actions

Answer: B

Explanation:

According to GDPR Article 39(1), the DPO's role is to monitor compliance, provide advice, and act as a point of contact for supervisory authorities. However, the DPO should not directly implement action plans, as this could create a conflict of interest (Recital 97). The responsibility for implementation lies with the controller or relevant departments, while the DPO ensures that the corrective actions align with GDPR requirements.

NEW QUESTION # 41

Why should the controller implement appropriate technical and organizational measures?

- A. To enable the processor to create and improve security features
- B. To maximize the processing of personal data
- C. To allow the data subject to monitor the processing of their personal data

Answer: C

Explanation:

GDPR Article 25 requires controllers to implement appropriate measures ensuring data protection. This includes transparency measures that allow data subjects to monitor the processing of their personal data, fulfilling their rights under Articles 12-22.

NEW QUESTION # 42

Scenario 7: EduCCS is an online education platform based in Netherlands. EduCCS helps organizations find, manage, and deliver their corporate training. Most of EduCCS's clients are EU residents. EduCCS is one of the few education organizations that have achieved GDPR compliance since 2019. Their DPO is a full-time employee who has been engaged in most data protection processes within the organization. In addition to facilitating GDPR compliance, the DPO acts as an intermediary point between EduCCS and other relevant interested parties. EduCCS's users can benefit from the variety of up-to-date training library and the possibility of accessing it through their phones, tablets, or computers. EduCCS's services are offered through two main platforms: online learning and digital training. To use one of these platforms, users should sign on EduCCS's website by providing their personal information. Online learning is a platform in which employees of other organizations can search for and request the training they need. Through its digital training platform, on the other hand, EduCCS manages the entire training and education program for other organizations.

Organizations that need this type of service need to provide information about their core activities and areas where training sessions are needed. This information is then analyzed by EduCCS and a customized training program is provided. In the beginning, all IT-related services were managed by two employees of EduCCS.

However, after acquiring a large number of clients, managing these services became challenging. That is why EduCCS decided to outsource the IT service function to X-Tech. X-Tech provides IT support and is responsible for ensuring the security of EduCCS's network and systems. In addition, X-Tech stores and archives EduCCS's information including their training programs and clients' and employees' data. Recently, X-Tech made headlines in the technology press for being a victim of a phishing attack. A group of three attackers hacked X-Tech's systems via a phishing campaign which targeted the employees of the Marketing Department. By compromising X-Tech's mail server, hackers were able to gain access to more than 200 computer systems. Consequently, access to the networks of EduCCS's clients was also allowed. Using EduCCS's employee accounts, attackers installed a remote access tool on EduCCS's compromised systems.

By doing so, they gained access to personal information of EduCCS's clients, training programs, and other information stored in its online payment system. The attack was detected by X-Tech's system administrator.

After detecting unusual activity in X-Tech's network, they immediately reported it to the incident management team of the company. One week after being notified about the personal data breach, EduCCS communicated the incident to the supervisory authority with a document that outlined the reasons for the delay revealing that due to the lack of regular testing or modification, their incident response plan was not adequately prepared to handle such an attack. Based on this scenario, answer the following question:

Question:

Should EduCCS document information related to the personal data breach, including facts, its impact, and the remedial action taken?

- A. No, EduCCS must report the breach only if more than 100,000 individuals were affected.
- B. No, EduCCS was not the direct target of the attack, so it cannot document details about the breach, its impact, or remedial actions.
- C. Yes, EduCCS should document the personal data breach to allow the supervisory authority to determine if the breach must be communicated to data subjects.

- D. Yes, EduCCS should document any personal data breach to enable the supervisory authority to verify compliance with GDPR's Article 33(Notification of a personal data breach to the supervisory authority).

Answer: D

Explanation:

Under Article 33(5) of GDPR, controllers must document personal data breaches, including their effects and corrective measures, even if notification to data subjects is not required.

- * Option A is correct because documentation is mandatory for compliance verification.
- * Option B is incorrect because documentation is required regardless of whether notification to data subjects is necessary.
- * Option C is incorrect because EduCCS, as the controller, is responsible for breach documentation.
- * Option D is incorrect because GDPR does not impose a breach reporting threshold based on the number of affected individuals.

References:

- * GDPR Article 33(5)(Documentation of breaches)
- * Recital 85(Controllers must record breaches and mitigation actions)

NEW QUESTION # 43

Question:

What is the role of the DPO in a DPIA?

- A. Approve the DPIA and ensure all risks are eliminated.
- B. Determine if a DPIA is necessary.
- C. Record the DPIA outcomes.
- D. Conduct the DPIA.

Answer: B

Explanation:

Under Article 39(1)(c) of GDPR, the DPO advises on the necessity of conducting a DPIA but does not conduct it themselves.

The controller is responsible for carrying out the DPIA.

- * Option B is correct because the DPO must determine whether a DPIA is required and provide recommendations.
- * Option A is incorrect because conducting the DPIA is the responsibility of the controller, not the DPO.
- * Option C is incorrect because while the DPO can assist, DPIA documentation is the controller's duty.
- * Option D is incorrect because DPOs advise but do not approve or eliminate all risks - risk management remains the responsibility of the controller.

References:

- * GDPR Article 39(1)(c)(DPO advises on DPIA necessity)
- * Recital 97(DPOs provide oversight, not execution)

NEW QUESTION # 44

.....

The advantages of our GDPR study materials are plenty and the price is absolutely reasonable. The clients can not only download and try out our products freely before you buy them but also enjoy the free update and online customer service at any time during one day. The clients can use the practice software to test if they have mastered the GDPR Study Materials and use the function of stimulating the test to improve their performances in the real test. So our products are absolutely your first choice to prepare for the test GDPR certification.

GDPR Reliable Test Labs: <https://www.pdfvce.com/PECB/GDPR-exam-pdf-dumps.html>

PECB Pdf GDPR Exam Dump Keep confident and optimistic, Here is the procedure to download your product: Go to www.PDFVCE.com Find 'Sign in to PDFVCE GDPR Reliable Test Labs' form (top-right corner), All in all, GDPR Reliable Test Labs - PECB Certified Data Protection Officer updated study material is really thinking for your convenience, PECB Pdf GDPR Exam Dump Moreover, you have to give consideration to your job or school task.

When each tab is clicked, the window the tab Pdf GDPR Exam Dump represents is opened, Is the foundation exam Effective, Keep confident and optimistic, Here is the procedure to download your product: Exam GDPR Vce Format Go to www.PDFVCE.com Find 'Sign in to PDFVCE' form (top-right corner).

The Best Pdf GDPR Exam Dump | Realistic GDPR Reliable Test Labs and New Valid PECB Certified Data Protection Officer Exam Online

All in all, Privacy And Data Protection PECB Certified Data Protection Officer updated study material GDPR is really thinking for your convenience, Moreover, you have to give consideration to your job or school task.

Our GDPR preparation exam have assembled a team of professional experts incorporating domestic and overseas experts and scholars to research and design related exam bank, committing great efforts to work for our candidates.

BTW, DOWNLOAD part of PDFVCE GDPR dumps from Cloud Storage: <https://drive.google.com/open?id=1OhfK1zEGhX3kKpDgJFenq6taKUsinyg>