Latest GDPR Exam Forum & Reliable GDPR Test Forum

DOWNLOAD the newest PracticeDump GDPR PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1baaxpuIdIu9CffMeFRPZUEnTpIdvh7Nm

The PECB GDPR exam dumps features are a free demo download facility, real, updated, and error-free PECB GDPR test questions, 1 year free updated PECB Certified Data Protection Officer (GDPR) exam questions and availability of PECB GDPR real questions in three different formats. PECB PDF Questions format, web-based practice test, and desktop-based GDPR Practice Test formats. All these three PECB GDPR exam dumps formats features surely will help you in preparation and boost your confidence to pass the challenging PECB Certified Data Protection Officer (GDPR) exam with good scores.

PECB GDPR Exam Syllabus Topics:

Topic	Details
Topic 1	• Data protection concepts: General Data Protection Regulation (GDPR), and compliance measures
Topic 2	• 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.
Topic 3	• 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.
Topic 4	• 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.

>> Latest GDPR Exam Forum <<

Quiz Updated PECB - GDPR - Latest PECB Certified Data Protection Officer Exam Forum

GDPR exam material before purchase; this will help you to figure out what the actual product will offer you and whether these features will help a prospective user to learn within a week. Also, upon purchase, the candidate will be entitled to 1 year free

updates, which will help candidates to stay up-to-date with GDPR news feeds and don't leave any chance which can cause their failure. The 100% refund policy is offered to all esteemed users, in the case for any reason, any candidates fail in GDPR certification exam so he may claim the refund.

PECB Certified Data Protection Officer Sample Questions (Q40-Q45):

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 in 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:
Based on scenario 9, the supervisory authority requested the conduct of a data protection audit in Soin without early notice. Is this acceptable?

- A. Yes, the supervisory authority may perform external audits randomly or after notification of the occurrence of a data breach in the company
- B. No, the supervisory authority can conduct a data protection external audit only if it is requested by the controller
- C. No, the supervisory authority may perform only scheduled external audits with at least two weeks' notice after the occurrence of a data breach in the company

Answer: A

Explanation:
Under GDPR Article 58(1)(b) and (d), supervisory authorities have the power to carry out data protection audits at their discretion. They do not need prior approval from the controller and may act proactively to ensure compliance. Supervisory authorities can investigate companies evenwithout a data breach, especially if there are concerns about GDPR compliance.

NEW QUESTION # 41
Scenario1:
MED is a healthcare provider located in Norway. It provides high-quality and affordable healthcare services, including disease prevention, diagnosis, and treatment. Founded in 1995, MED is one of the largest health organizations in the private sector. The company has constantly evolved in response to patients' needs.
Patients that schedule an appointment in MED's medical centers initially need to provide their personal information, including name, surname, address, phone number, and date of birth. Further checkups or admission require additional information, including previous

medical history and genetic data. When providing their personal data, patients are informed that the data is used for personalizing treatments and improving communication with MED's doctors. Medical data of patients, including children, are stored in the database of MED's health information system. MED allows patients who are at least 16 years old to use the system and provide their personal information independently. For children below the age of 16, MED requires consent from the holderof parental responsibility before processing their data.
MED uses a cloud-based application that allows patients and doctors to upload and access information.
Patients can save all personal medical data, including test results, doctor visits, diagnosis history, and medicine prescriptions, as well as review and track them at any time. Doctors, on the other hand, can access their patients' data through the application and can add information as needed.
Patients who decide to continue their treatment at another health institution can request MED to transfer their data. However, even if patients decide to continue their treatment elsewhere, their personal data is still used by MED. Patients' requests to stop data processing are rejected. This decision was made by MED's top management to retain the information of everyone registered in their databases.
The company also shares medical data with InsHealth, a health insurance company. MED's data helps InsHealth create health insurance plans that meet the needs of individuals and families.
MED believes that it is its responsibility to ensure the security and accuracy of patients' personal data. Based on the identified risks associated with data processing activities, MED has implemented appropriate security measures to ensure that data is securely stored and processed.
Since personal data of patients is stored and transmitted over the internet, MED uses encryption to avoid unauthorized processing, accidental loss, or destruction of data. The company has established a security policy to define the levels of protection required for each type of information and processing activity. MED has communicated the policy and other procedures to personnel and provided customized training to ensure proper handling of data processing.
Question:
Based on scenario 1, MED shares patients' personal data with a health insurance company. Does MED comply with thepurpose limitation principle?

- A. Yes, personal data may be used for purposes in the public interest or statistical purposes in accordance withArticle 89 of GDPR.
- B. Yes, as long as the data is encrypted before sharing.
- C. Yes, using personal data for creating health insurance plans is within the scope of the data collection purpose.
- D. No, personal data should be collected for specified, explicit, and legitimate purposes in accordance with Article 5 of GDPR.

Answer: D

NEW QUESTION # 42
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:
Is the transfer of data fromBerc to Untyin compliance with GDPR?

- A. No, Berc must conduct a new DPIA before transferring data to Switzerland.
- B. Yes, Berc can transfer data to Unty because Switzerland provides a level of data protection that is "essentially equivalent" to that of the EU.

- C. Yes, Berc can transfer data to Unty because they collected data for the same purpose.
- D. No, Berc cannot transfer data to a company in Switzerland unless authorization from the supervisory authority in France is obtained.

Answer: B

Explanation:
UnderArticle 45 of GDPR,data transfers to third countriesare lawful if the European Commission has adopted an adequacy decision, meaning the countryoffers equivalent protection to GDPR. Switzerland has such an adequacy decision, makingBerc's transfer lawful.
* Option A is correctbecause Switzerlandmeets GDPR adequacy standards.
* Option B is incorrectbecausehaving the same purpose does not automatically make the transfer lawful.
* Option C is incorrectbecauseno supervisory authorization is neededwhen an adequacy decision exists.
* Option D is incorrectbecausea 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

NEW QUESTION # 43
Why should the controller implement appropriate technical and organizational measures?

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

Answer: B

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 # 44
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 in 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:
Can the DPO appointed by Soin carry out the data protection external audit requested by the supervisory authority?

- A. Yes, data protection external audits should be conducted by auditors contracted by Soin who can be employees of the company
- B. No, data protection external audits should be conducted by independent auditors who are not part of the company being audited
- C. Yes, Soin's DPO is allowed to conduct a data protection external audit but only if requested by the supervisory authority

Answer: B

Explanation:
GDPR Article 58(1) gives supervisory authorities the power to conduct external audits, which mustbe independent and unbiased. A company's internal DPO cannot conduct an external audit, as this would pose a conflict of interest (Recital 97). External audits should be conducted by supervisory authorities or third-party auditors, ensuring objectivity.

NEW QUESTION # 45
.....