Latest GDPR Exam Testking - GDPR Pass Leader Dumps

Up to now, we have business connection with tens of thousands of exam candidates who adore the quality of our GDPR exam questions. Besides, we try to keep our services brief, specific and courteous with reasonable prices of GDPR Study Guide. All your questions will be treated and answered fully and promptly. So as long as you contact us to ask for the questions on the GDPR learning guide, you will get the guidance immediately.

PECB GDPR Exam Syllabus Topics:

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

>> Latest GDPR Exam Testking <<

PECB GDPR Pass Leader Dumps | GDPR Reliable Exam Review

Are you still satisfied with your present job? Do you still have the ability to deal with your job well? Do you think whether you have the competitive advantage when you are compared with people working in the same field? If your answer is no， you are a right place now. Because our GDPR Exam Torrent will be your good partner and you will have the chance to change your work which you are not satisfied with, and can enhance your ability by our GDPR guide questions, you will pass the exam and achieve your target.

PECB Certified Data Protection Officer Sample Questions (Q63-Q68):

NEW QUESTION # 63
Question:
Which of the following options is theDPO's responsibilitywhen processing personal datarelated to criminal convictionsis carried out by anofficial authority?

- A. Determiningthe location where sensitive data may be processed.
- B. Approvingall security measures for processingthis data.
- C. Ensuringcompliance with any legal requirementsof Member States.
- D. Assessingthe necessity of knowing a data subject's identity.

Answer: C

Explanation:
UnderArticle 39(1)(b) of GDPR, the DPOmonitors compliancewith GDPRand other applicable laws, includingMember State lawsoncriminal conviction data.
* Option C is correctbecauseDPOs must ensure processing aligns with national legal requirements.
* Option A is incorrectbecausedetermining processing locationsis atechnical decision, not aDPO responsibility.
* Option B is incorrectbecauseDPOs do not assess the necessity of identity disclosure.
* Option D is incorrectbecauseapproving security measures is the responsibility of controllers and processors, not the DPO.
References:
* GDPR Article 39(1)(b)(DPO's role in ensuring legal compliance)
* Recital 97(DPO responsibilities in public and private sectors)

NEW QUESTION # 64
Scenario3:
COR Bank is an international banking group that operates in 31 countries. It was formed as the merger of two well-known investment banks in Germany. Their two main fields of business are retail and investment banking. COR Bank provides innovative solutions for services such as payments, cash management, savings, protection insurance, and real-estate services. COR Bank has a large number of clients and transactions.
Therefore, they process large information, including clients' personal data. Some of the data from the application processes of COR Bank, including archived data, is operated by Tibko, an IT services company located in Canada. To ensure compliance with the GDPR, COR Bank and Tibko have reached a data processing agreement Based on the agreement, the purpose and conditions of data processing are determined by COR Bank. However, Tibko is allowed to make technical decisions for storing the data based on its own expertise. COR Bank aims to remain a trustworthy bank and a long-term partner for its clients. Therefore, they devote special attention to legal compliance. They started the implementation process of a GDPR compliance program in 2018. The first step was to analyze the existing resources and procedures. Lisa was appointed as the data protection officer (DPO). Being the information security manager of COR Bank for many years, Lisa had knowledge of the organization's core activities. She was previously involved in most of the processes related to information systems management and data protection. Lisa played a key role in achieving compliance to the GDPR by advising the company regarding data protection obligations and creating a data protection strategy. After obtaining evidence of the existing data protection policy, Lisa proposed to adapt the policy to specific requirements of GDPR. Then, Lisa implemented the updates of the policy within COR Bank. To ensure consistency between processes of different departments within the organization, Lisa has constantly communicated with all heads of GDPR. Then, Lisa implemented the updates of the policy within COR Bank. To ensure consistency between processes of different departments within the organization, Lisa has constantly communicated with all heads of departments. As the DPO, she had access to several departments,including HR and Accounting Department. This assured the organization that there was a continuous cooperation between them. The activities of some departments within COR Bank are closely related to data protection. Therefore, considering their expertise, Lisa was advised from the top management to take orders from the heads of those departments when taking decisions related to their field. Based on this scenario, answer the following question:
Question:
According to scenario 3,Lisa was appointed as the Data Protection Officer (DPO)of COR Bank. Is this action in compliance with GDPR?

- A. No, Lisa cannot be appointed as a DPO because she was already an information security officer.
- B. Yes, the DPO may be a staff member of the controller or processor or fulfill the tasks based on a service contract.
- C. No, an external DPO must be contracted when personal data is collected or processed by an organization that is not established in the European Union.
- D. Yes, the DPO must be a staff member of the controller or processor in all cases when processing includes special categories of data.

Answer: B

Explanation:
UnderArticle 37(6) of GDPR, theDPO can be an employeeof the company oran external contractor. Lisa's appointmentcomplieswith GDPR because she is a staff member withdata protection expertise.
* Option A is correctbecause GDPR allows organizations to appoint aninternal or external DPO.
* Option B is incorrectbecause a DPOdoes not have to be an internal staff membereven for special categories of data.
* Option C is incorrectbecause a company canappoint an internal DPO even if it operates internationally.
* Option D is incorrectbecause having another roledoes not disqualify someone from being a DPO, as long as there isno conflict of interest.
References:
* GDPR Article 37(6)(DPO may be an employee or external contractor)
* Recital 97(DPO qualifications and independence)

NEW QUESTION # 65
Scenario 8:MA store is an online clothing retailer founded in 2010. They provide quality products at a reasonable cost. One thing that differentiates MA store from other online shopping sites is their excellent customer service.
MA store follows a customer-centered business approach. They have created a user-friendly website with well-organized content that is accessible to everyone. Through innovative ideas and services, MA store offers a seamless user experience for visitors while also attracting new customers. When visiting the website, customers can filter their search results by price, size, customer reviews, and other features. One of MA store's strategies for providing, personalizing, and improving its products is data analytics. MA store tracks and analyzes the user actions on its website so it can create customized experience for visitors.
In order to understand their target audience, MA store analyzes shopping preferences of itscustomers based on their purchase history. The purchase history includes the product that was bought, shipping updates, and payment details. Clients' personal data and other information related to MA store products included in the purchase history are stored in separate databases. Personal information, such as clients' address or payment details, are encrypted using a public key. When analyzing the shopping preferences of customers, employees access only the information about the product while the identity of customers is removed from the data set and replaced with a common value, ensuring that customer identities are protected and cannot be retrieved.
Last year, MA store announced that they suffered a personal data breach where personal data of clients were leaked. The personal data breach was caused by an SQL injection attack which targeted MA store's web application. The SQL injection was successful since no parameterized queries were used.
Based on this scenario, answer the following question:
According to scenario 8, MA store analyzed shopping preferences of its customers by analyzing the product they have bought in the customer's purchase history. Which option is correct in this case?

- A. MA store can use this type of information only during the period for which data subjects have given consent
- B. MA store can use this type of information for an indefinite period of time since it is anonymized
- C. MA store can use this type of information for a limited period of time since it is pseudonymized

Answer: C

Explanation:
Since the data is pseudonymized (not fully anonymized), it remains personal data under GDPR and cannot be retained indefinitely. Article 5(1)(e) of GDPR states that personal data must be kept only for as long as necessary for the intended processing purpose. Additionally, Recital 26 of GDPR clarifies that pseudonymized data is still considered personal data if re-identification is possible. Therefore, MA Store must implement a retention policy that ensures the data is deleted or further anonymized once it is no longer needed for analysis.

NEW QUESTION # 66
Scenario:2
Soyled is a retail company that sells a wide range of electronic products from top European brands. It primarily sells its products in its online platforms (which include customer reviews and ratings), despite using physical stores since 2015. Soyled's website and mobile app are used by millions of customers. Soyled has employed various solutions to create a customer-focused ecosystem and facilitate growth. Soyled uses customer relationship management (CRM) software to analyze user data and administer the interaction with customers. The software allows the company to store customer information, identify sales opportunities, and manage marketing campaigns. It automatically obtains information about each user's IP address and web browser cookies. Soyled also uses the software to collect behavioral data, such as users' repeated actions and mouse movement information. Customers must create an account to buy from Soyled's online platforms. To do so, they fill out a standard sign-up form of three mandatory boxes (name, surname, email address) and a non-mandatory one (phone number). When the user clicks the email address box, a pop-up message appears as follows: "Soyled needs your email address to grant you access to your account and contact you about any changes

related to your account and our website. For further information, please read our privacy policy.' When the user clicks the phone number box, the following message appears: "Soyled may use your phone number to provide text updates on the order status. The phone number may also be used by the shipping courier." Once the personal data is provided, customers create a username and password, which are used to access Soyled's website or app. When customers want to make a purchase, they are also required to provide their bank account details. When the user finally creates the account, the following message appears: "Soyled collects only the personal data it needs for the following purposes: processing orders, managing accounts, and personalizing customers' experience. The collected data is shared with our network and used for marketing purposes." Soyled uses personal data to promote sales and its brand. If a user decides to close the account, the personal data is still used for marketing purposes only. Last month, the company received an email from John, a customer, claiming that his personal data was being used for purposes other than those specified by the company. According to the email, Soyled was using the data for direct marketing purposes. John requested details on how his personal data was collected, stored, and processed. Based on this scenario, answer the following question:
Question:
The GDPR indicates that the processing of personal data should be based on alegal contractwith the data subject. Based on scenario 6, has Soyled fulfilled this requirement?

- A. No, because Soyled did not obtain explicit consent for data processing.
- B. No, data subjects are informed that the personal data will be shared with Soyled's networkonly afterthe personal data is collected.
- C. Yes, once the account is created, Soyled informs its customers that their personal data will be shared with the network.
- D. Yes, data subjects are informed about the purpose of collecting the email address and phone number before the data is collected.

Answer: B

Explanation:
UnderArticle 6(1) of GDPR, processing personal data must have alawful basis, such as consent, contract, legal obligation, or legitimate interest. Additionally, underArticle 13, controllers must inform usersbefore collecting their data.
Soyledfailed to disclosethat personal data would be shared with the networkbefore collection, whichviolates GDPR transparency requirements.Option C is correct.Option Ais incorrect because informing about email collection does not mean lawful processing.Option Bis incorrect because the information was not disclosed at the right time.Option Dis incorrect because explicit consent is not necessarily required if another lawful basis applies.
References:
* GDPR Article 6(1)(Lawfulness of processing)
* GDPR Article 13(1)(Transparency in data processing)

NEW QUESTION # 67
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 theirpersonal 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 holder of 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, which data subject right isNOTguaranteed by MED?

- A. Right to data portability
- B. Right to be informed
- C. Right to rectification
- D. Right to restriction of processing

Answer: D

Explanation:
UnderArticle 18 of GDPR, theright to restriction of processingallows data subjects to request that processing of their personal data be limited under certain conditions, such as when accuracy is contested or processing is unlawful but the data subject opposes erasure.
From the scenario, MEDdoes not provide the option to restrict processing, as patients who request to stop processing are denied. This makesOption Bcorrect.Option Ais incorrect because MED does inform patients about data collection purposes.Option Cis incorrect because medical data could be transferred to other institutions.Option Dis incorrect because rectification of inaccurate data is a standard obligation.
References:
* GDPR Article 18(Right to restriction of processing)
* GDPR Article 12(Transparent communication with data subjects)

NEW QUESTION # 68
.....

myportal.utt.edu.tt, classesarefun.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, vietnamfranchise.vn, myportal.utt.edu.tt, Disposable vapes