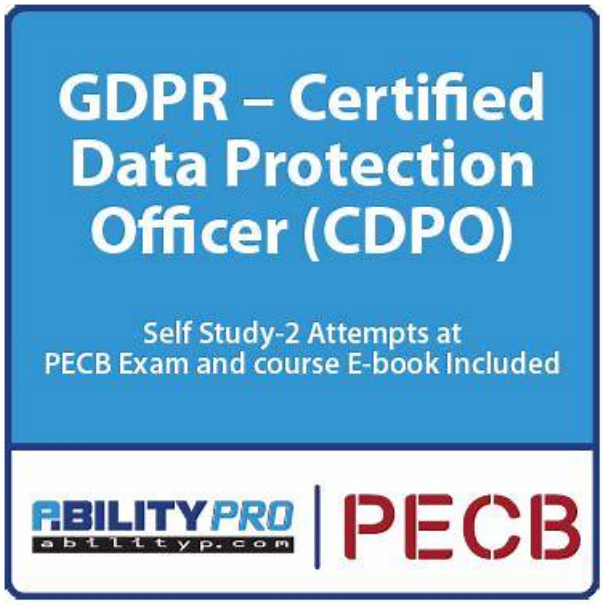
Best way to practice test for PECB GDPR?



BONUS!!! Download part of Actual4dump GDPR dumps for free: https://drive.google.com/open?id=1c-6zztwV-axkgyIkRFPZUzIiIsSVIoGo

No matter you are a fresh man or experienced IT talents, here, you may hear that GDPR certifications are designed to take advantage of specific skills and enhance your expertise. While, if you want to be outstanding in the crowd, it is better to get the GDPR certification. While, where to find the latest GDPR Study Material for preparation is another question. PECB GDPR exam training will guide you and help you to get the GDPR certification. Hurry up, download GDPR test practice torrent for free, and start your study at once.

PECB GDPR Exam Syllabus Topics:

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

>> Pass4sure GDPR Pass Guide <<

Latest PECB GDPR Braindumps Pdf, GDPR Exam Questions And Answers

As the rapid development of the world economy and intense competition in the international, the leading status of knowledge-based economy is established progressively. A lot of people are in pursuit of a good job, a GDPR certification, and a higher standard of life. You just need little time to download and install it after you purchase, then you just need spend about 20~30 hours to learn it. We are glad that you are going to spare your precious time to have a look to our GDPR Exam Guide.

PECB Certified Data Protection Officer Sample Questions (Q43-Q48):

NEW QUESTION # 43
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 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 andprocessing 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, is the processing of children's personal data performed by MED in compliance with GDPR?

- A. Yes, as long as the processing is conducted with industry-standard encryption.
- B. No, MED must obtain explicit consent from the child, regardless of parental consent, for the processing to be in compliance with GDPR.
- C. No, the processing of personal data of children below the age of 16 years is not in compliance with the GDPR, even if parental consent is provided.
- D. Yes, the processing of children's personal data below the age of 16 years with parental consent is in compliance with GDPR.

Answer: D

Explanation:
UnderArticle 8 of the GDPR, the processing of personal data of children under 16 years is only lawful if parental or guardian consent is obtained. However, Member States can lower the age limit to 13 years if they choose.
In this scenario, MED requires parental consent for children below 16 years, which aligns with GDPR requirements.
Therefore,Option Bis correct.Option Ais incorrect because GDPR allows parental consent.

Option Cis incorrect because GDPR does not require explicit consent from the child when parental consent is given.Option Dis incorrect because encryption alone does not determine compliance.
References:
* GDPR Article 8(Conditions for children's consent)
* Recital 38(Protection of children's data)

NEW QUESTION # 44
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 canbenefit 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:
ShouldEduCCS document information related to the personal data breach, includingfacts, its impact, and the remedial action taken?

- A. Yes, EduCCS should document the personal data breachto allow the supervisory authority to determine if the breach must be communicated to data subjects.
- B. No, EduCCS wasnot the direct target of the attack, so itcannot document details about the breach, its impact, or remedial actions.
- C. No, EduCCS must report the breachonly if more than 100,000 individuals were affected.
- D. Yes, EduCCS should document any personal data breachto enable the supervisory authority to verify compliancewithGDPR's Article 33(Notification of a personal data breach to the supervisory authority).

Answer: D

Explanation:
UnderArticle 33(5) of GDPR, controllers mustdocument personal data breaches, including their effects and corrective measures, even if notification to data subjects is not required.
* Option A is correctbecausedocumentation is mandatory for compliance verification.
* Option B is incorrectbecausedocumentation is required regardless of whether notification to data subjects is necessary.
* Option C is incorrectbecauseEduCCS, as the controller, is responsible for breach documentation.
* Option D is incorrectbecauseGDPR 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 # 45
Question:
What is themain purpose of conducting a DPIA?

- A. Toeliminate all risksassociated with processing personal data.
- B. Toextensively assess the impactsof the identified risks on individuals.
- C. Tomeasure the potential consequencesof the identified risks on the organization.
- D. Toidentify the causesof the identified risks.

Answer: B

Explanation:
UnderArticle 35 of GDPR, a DPIA's primary goal is toassess the risks to individuals' rights and freedoms arising from data processing.
* Option B is correctbecauseDPIAs focus on evaluating and mitigating risks to data subjects.
* Option A is incorrectbecauseDPIAs are not just about identifying causes but about assessing and mitigating risks.
* Option C is incorrectbecauseGDPR prioritizes risks to individuals, not just organizations.
* Option D is incorrectbecauseeliminating all risks is not possible-DPIAs aim to manage and minimize risks.
References:
* GDPR Article 35(1)(DPIA requirement for high-risk processing)
* Recital 84(DPIAs help protect individuals' rights)

NEW QUESTION # 46
Scenario:
Pinky, a retail company,received a requestfrom adata subjectto identify which purchasesthey had madeat differentphysical store locations. However,Pinky does not link purchase records to customer identities, since purchasesdo not require account creation.
Question:
Should Pinkyprocess additional informationfrom customers in order toidentify the data subjectas requested?

- A. Yes, Pinky is required tomaintain, acquire, or process additional informationin order to identify the data subject.
- B. No, Pinky isnot requiredto process additional information, since the processing of personal data in this case does not require Pinky toidentify the data subject.
- C. No, but Pinky must ask the data subject to provide further evidence proving their identity.
- D. Yes, Pinky is required to process additional information for the purpose ofexercising the data subject' s rightscovered inArticles 15-21 of GDPR.

Answer: B

Explanation:
UnderArticle 11(1) of GDPR, controllersare not required to process additional datafor the sole purpose of identifying data subjectsif such identification is not needed for processing.
* Option C is correctbecausePinky does not store identifiable purchase data, so it is not required to create additional records.
* Option A and B are incorrectbecauseGDPR does not obligate controllers to process additional data if identification is unnecessary.
* Option D is incorrectbecausePinky cannot require additional information when it does not have a basis to process identity-linked data.
References:
* GDPR Article 11(1)(Controllers are not required to process extra data for identification)
* Recital 57(Data controllers should avoid collecting unnecessary identity data)

NEW QUESTION # 47
Question:
In whichphase of the incident management planshould the process owner define theessential information needed for identifying and classifying security incidents, while thepoint of contact and response team conduct assessments and determine actions?

- A. Assessment and decision phase.
- B. Detection and reporting phase.
- C. Plan and prepare phase.
- D. Remediation and recovery phase.

Answer: A

Explanation:
TheAssessment and Decision Phaseis wherepotential security incidents are reviewed, classified, and appropriate response actions are determined.
* Option B is correctbecausethis phase focuses on analyzing threats and deciding how to mitigate risks.
* Option A is incorrectbecauseplanning and preparation occur before an incident is detected.
* Option C is incorrectbecausedetection focuses on identifying possible breaches, not classifying them.
* Option D is incorrectbecauseremediation happens after decisions on response actions have been made.
References:
* ISO/IEC 27035-1:2016(Incident management process stages)
* GDPR Article 32(1)(d)(Security measures should ensure quick response to incidents)

NEW QUESTION # 48
.....

Here in this Desktop practice test software, the PECB Certified Data Protection Officer (GDPR) practice questions given are very relevant to the actual PECB GDPR exam. It is compatible with Windows computers. Actual4dump provides its valued customers with customizable PECB Certified Data Protection Officer (GDPR) practice exam sessions. The PECB GDPR practice test software also keeps track of the previous PECB GDPR practice exam attempts.