GDPR Test Sample Questions - Exam GDPR Course

P.S. Free 2025 PECB GDPR dumps are available on Google Drive shared by TorrentVCE: https://drive.google.com/open?id=1hzCeEfImq15W1ugYTdSUaLaEghvwGcC2

Living in such a world where competitiveness is a necessity that can distinguish you from others, every one of us is trying our best to improve ourselves in every way. It has been widely recognized that the GDPR Exam can better equip us with a newly gained personal skill, which is crucial to individual self-improvement in today's computer era. With the certified advantage admitted by the test PECB certification, you will have the competitive edge to get a favorable job in the global market.

PECB GDPR Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• Data protection concepts: General Data Protection Regulation (GDPR), and compliance measures
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	• 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 Test Sample Questions <<

Exam GDPR Course, GDPR Valid Exam Labs

We don't want you to prepare and practice the old questions and waste time. Therefore, our team of certified experts includes updated PECB Certified Data Protection Officer GDPR Exam Questions as soon as they are released. TorrentVCE provides up-to-date PECB exam questions.

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

NEW QUESTION # 63
Scenario:
A financial institution collectsbiometric data of its clients, such asface recognition, to support apayment authentication processthat they recently developed. The institution ensures thatdata subjects provide explicit consentfor the processing of theirbiometric datafor this specific purpose.
Question:
Based on this scenario, should theDPO advise the organization to conduct a DPIA (Data Protection Impact Assessment)?

- A. Yes, but only if the biometric data is storedfor more than five years.
- B. No, because DPIAs areonly requiredwhen processing personal dataon a large scale, which is not specified in this case.
- C. No, becauseexplicit consenthas already been obtained from the data subjects.
- D. Yes, because biometric data is consideredspecial category personal data, and its processing is likely to involvehigh risk.

Answer: D

Explanation:
UnderArticle 35(3)(b) of GDPR, aDPIA is mandatoryfor processing that involveslarge-scale processing of special category data, including biometric data. Even ifexplicit consentis obtained,the risks associated with biometric processing require further evaluation.
* Option A is correctbecausebiometric data processing poses high risks to fundamental rights and freedoms, necessitating a DPIA.
* Option B is incorrectbecauseobtaining consent does not eliminate the requirement to conduct a DPIA.
* Option C is incorrectbecauseDPIAs are required for biometric processing regardless of scaleif risks are present.
* Option D is incorrectbecausestorage duration is not a determining factor for DPIA requirements.
References:
* GDPR Article 35(3)(b)(DPIA requirement for special category data)
* Recital 91(Processing biometric data requires special safeguards)

NEW QUESTION # 64
Scenario:
Amarketing companydiscovers that anunauthorized party accessed its customer database, exposing5,000 recordscontainingnames, email addresses, and phone numbers. The breach occurred due to a misconfigured server.
Question:
To comply withGDPR, whichinformation must the company includein itsnotification to the supervisory authority?

- A. Both A and B.
- B. Theapproximate number of data subjectsand records affected.
- C. Adescription of the natureof the personal data breach.
- D. Theidentity of the attackerand their potential motive.

Answer: A

Explanation:
UnderArticle 33(3) of GDPR, a breach notification to thesupervisory authoritymust include:
* The nature of the breach(what type of data was accessed).
* The number of affected individuals and records.
* The potential impact on data subjects.
* Measures taken to mitigate the breach.
* Option C is correctbecauseboth the nature of the breach and the number of affected individuals must be reported.
* Option A is incorrectbecausewhile the breach description is necessary, the number of affected individuals must also be included.
* Option B is incorrectbecausethe breach description is also required.
* Option D is incorrectbecauseidentifying the attacker is not required under GDPR.
References:
* GDPR Article 33(3)(Content requirements for breach notification)
* Recital 87(Timely reporting ensures risk mitigation)

NEW QUESTION # 65
Scenario:
An organization conducted anonline surveyto gather opinions onglobal warming. The survey collected personal data, includingage, nationality, gender, and city of residence.
Question:

What should be considered whenidentifying this processing activity?

- A. Thesurvey platform's technical security measures.
- B. Information on thepersonal data collectedand itssensitivity.
- C. Adescription of data subjectsand thecategories of personal datacollected.
- D. Information abouthow the data is processed.

Answer: C

Explanation:
UnderArticle 30 of GDPR, controllersmust maintain a record of processing activities, including the categories of data subjectsandtypes of personal data collected.
* Option C is correctbecausedescribing data subjects and personal data categories is fundamental in processing documentation.
* Option A is incorrectbecausesensitivity alone does not define processing obligations.
* Option B is incorrectbecauseprocessing methods are important but do not solely define processing activities.
* Option D is incorrectbecausetechnical security measures are relevant but are not part of defining processing activities.
References:
* GDPR Article 30(1)(b)(Controllers must document categories of data subjects and personal data processed)
* Recital 82(Proper record-keeping of processing activities)

NEW QUESTION # 66
Scenario5:
Recpond is a German employment recruiting company. Their services are delivered globally and include consulting and staffing solutions. In the beginning. Recpond 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. Recpond 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 Recpond. Recpond'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 Recpond's clients, who proceed with the recruitment process. Files of candidates that are not selected are stored in Recpond'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 Recpond, 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. Recpond, 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. Recpond 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 Recpond.Based on this scenario, answer the following question:
Question:
Recpondstores files of candidates who are not selectedin its databases,even if they withdraw consent. Is this acceptable under GDPR?

- A. No, Recpond must retain candidate data for statistical analysis but must anonymize it.
- B. Yes, the GDPR allows personal data to be processedeven after consent is withdrawnso organizations can use the data for future recruitment opportunities.
- C. Yes, the GDPR only requires the controller tostop processing the datawhen consent is withdrawn but does not require its deletion.
- D. No, the GDPR requires the controller to erase personal data if the data subject withdraws their consent for data processing.

Answer: D

NEW QUESTION # 67

Question:
What is therole of the DPO in a DPIA?

- A. Conductthe DPIA.
- B. Determineif a DPIA is necessary.
- C. Recordthe DPIA outcomes.
- D. Approvethe DPIA and ensure all risks are eliminated.

Answer: B

Explanation:
UnderArticle 39(1)(c) of GDPR, theDPO advises on the necessity of conducting a DPIAbut doesnot conduct it themselves. Thecontroller is responsiblefor carrying out the DPIA.
* Option B is correctbecausethe DPO must determine whether a DPIA is required and provide recommendations.
* Option A is incorrectbecauseconducting the DPIA is the responsibility of the controller, not the DPO.
* Option C is incorrectbecausewhile the DPO can assist, DPIA documentation is the controller's duty.
* Option D is incorrectbecauseDPOs 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 # 68
.....

BTW, DOWNLOAD part of TorrentVCE GDPR dumps from Cloud Storage: https://drive.google.com/open?id=1hzCeEfImq15W1ugYTdSUaLaEghvwGcC2