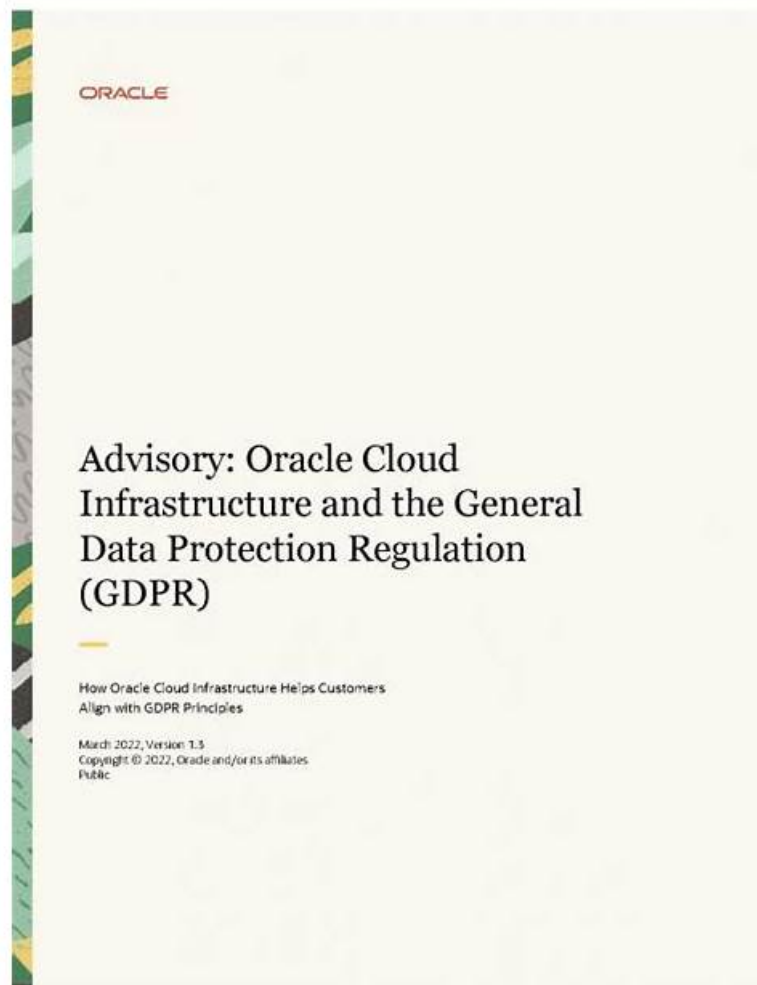


GDPR Instant Access, GDPR Updated Dumps



P.S. Free & New GDPR dumps are available on Google Drive shared by PrepPDF: <https://drive.google.com/open?id=1InlPtG3flePESoDWBmliZHsiNEjBw8L>

At PrepPDF, we strive hard to offer a comprehensive PECB Certified Data Protection Officer (GDPR) exam questions preparation material bundle pack. The product available at PrepPDF includes PECB GDPR Real Dumps pdf and mock tests (desktop and web-based). Practice exams give an experience of taking the PECB Certified Data Protection Officer (GDPR) actual exam.

To maximize your chances of your success in the GDPR Certification Exam, our company introduces you to an innovatively created exam testing tool-our GDPR exam questions. Not only that you will find that our GDPR study braindumps are full of the useful information in the real exam, but also you will find that they have the function to measure your level of exam preparation and cover up your deficiency before appearing in the actual exam.

>> GDPR Instant Access <<

GDPR Updated Dumps, Exam Dumps GDPR Zip

In this competitive IT industry, having some authentication certificate can help you promote job position. Many companies that take a job promotion or increase salary for you will refer to how many gold content your authentication certificates have. PECB GDPR is a high gold content certification exam. PECB GDPR authentication certificate can meet many IT employees' needs. PrepPDF can provide you with PECB certification GDPR exam targeted training. You can free download PrepPDF's trial version of raining tools and some exercises and answers about PECB certification GDPR exam as a try.

PECB Certified Data Protection Officer Sample Questions (Q32-Q37):

NEW QUESTION # 32

Scenario5:

Repond is a German employment recruiting company. Their services are delivered globally and include consulting and staffing solutions. In the beginning, Repond 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. Repond 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 Repond. Repond'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 Repond's clients, who proceed with the recruitment process. Files of candidates that are not selected are stored in Repond'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 Repond, 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. Repond, 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, Repond 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 Repond. Based on this scenario, answer the following question:

Question:

Which statement regarding the material scope of the GDPR is incorrect?

- A. The GDPR does not apply to the processing of personal data by Member States when carrying out activities that fall within the scope of the Treaty on European Union (TEU).
- B. The GDPR applies to the processing of personal data by a company established in the EEA, even if the data subjects are located outside the EEA.
- **C. The GDPR applies to the processing of personal data in the course of an activity that falls outside the scope of Union law.**
- D. The GDPR applies to the processing of personal data wholly or partly by automated means.

Answer: C

Explanation:

The material scope of the GDPR is outlined in Article 2. It applies to the processing of personal data by automated means and to non-automated processing if the data is part of a filing system. The GDPR does not apply to activities outside the scope of Union law, such as national security activities, which are excluded under Recital 16.

* Option B is correct because the GDPR does not apply to activities falling outside the scope of Union law, such as law enforcement operations covered by the Law Enforcement Directive (EU 2016/680).

* Option A is incorrect because automated processing is explicitly covered by GDPR.

* Option C is incorrect because data processing by Member States under TEU (e.g., national security and defense) is excluded.

* Option D is incorrect because GDPR applies to controllers/processors established in the EEA, even if data subjects are outside the EEA (Article 3(1)).

References:

* GDPR Article 2(2)(a) (Exclusion of activities outside EU law)

* GDPR Article 3(1) (Territorial scope)

* Recital 16 (GDPR does not apply to national security)

NEW QUESTION # 33

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 departments. 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, Tibko stores archived data on behalf of COR Bank. This means that Tibko is a:

- A. Joint controller with COR Bank, since they archive COR Bank's data and take technical decisions regarding data protection.
- **B. Data processor, since they store COR Bank's data based on the purpose and conditions defined by COR Bank.**
- C. Data controller, since they control some of the data from the application processes of COR Bank.
- D. Independent controller, since Tibko handles data security and storage.

Answer: B

Explanation:

Under Article 4(8) of GDPR, a data processor processes personal data on behalf of a controller and does not determine the purpose of processing. Tibko only stores and manages data but does not decide why it is processed.

* Option B is correct because Tibko acts as a processor for COR Bank.

* Option A is incorrect because Tibko does not determine data processing purposes.

* Option C is incorrect because joint controllers must jointly decide on processing purposes.

* Option D is incorrect because Tibko does not act as an independent controller.

References:

* GDPR Article 4(8) (Definition of a processor)

* GDPR Article 28 (Processor obligations)

NEW QUESTION # 34

Scenario 5:

Repond is a German employment recruiting company. Their services are delivered globally and include consulting and staffing solutions. In the beginning, Repond 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. Repond 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 Repond. Repond'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 Repond's clients, who proceed with the recruitment process. Files of candidates that are not selected are stored in Repond'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 Repond, 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. Repond, 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:

Recpond stores files of candidates who are not selected in its databases, even if they withdraw consent. Is this acceptable under GDPR?

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

Answer: B

Explanation:

Under Article 17 of GDPR (Right to Erasure), data subjects have the right to request deletion of their personal data when consent is withdrawn, unless a legal obligation or legitimate interest requires retention.

* Option A is correct because Recpond must erase personal data if consent is withdrawn and no other lawful basis exists.

* Option B is incorrect because GDPR requires deletion, not just stopping processing.

* Option C is incorrect because organizations cannot retain data for future purposes without an explicit legal basis.

* Option D is incorrect because statistical use must involve anonymization, which is not mentioned in Recpond's process.

References:

* GDPR Article 17(1)(b) (Right to be forgotten when consent is withdrawn)

* Recital 65 (Obligation to erase personal data when processing is no longer necessary)

NEW QUESTION # 35

Scenario 3:

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 departments. 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:

Considering the GDPR's territorial scope and the data processing agreement between COR Bank and Tibko, which of the following best describes Tibko's obligations under the GDPR?

- A. Tibko is not subject to GDPR since it is located outside the EU and only provides IT services.

- B. Tibko's compliance with GDPR is limited to implementing technical safeguards for data storage, as stipulated by the data processing agreement with COR Bank.
- **C. Tibko is required to comply with the GDPR because it processes personal data on behalf of COR Bank, and COR Bank determines the purpose of processing under their agreement.**
- D. Tibko must adhere to all GDPR provisions independently, including determining the purpose of processing personal data, as a processor acting under COR Bank's authority.

Answer: C

Explanation:

Under Article 3(2) of GDPR, GDPR applies extraterritorially if an entity outside the EU processes personal data of EU residents on behalf of a controller subject to GDPR. Tibko processes COR Bank's client data, making it subject to GDPR as a processor under Article 28.

- * Option C is correct because Tibko must comply with GDPR since it processes EU data on behalf of COR Bank.
- * Option A is incorrect because processors must comply with broader GDPR obligations, not just technical safeguards.
- * Option B is incorrect because processors do not determine the purpose of processing; that is the controller's responsibility.
- * Option D is incorrect because location outside the EU does not exempt processors from GDPR obligations.

References:

- * GDPR Article 3(2)(Territorial Scope)
- * GDPR Article 28(1)(Processor obligations)
- * Recital 81(Processor responsibilities)

NEW QUESTION # 36

Scenario:

A financial institution collects biometric data of its clients, such as face recognition, to support a payment authentication process that they recently developed. The institution ensures that data subjects provide explicit consent for the processing of their biometric data for this specific purpose.

Question:

Based on this scenario, should the DPO advise the organization to conduct a DPIA (Data Protection Impact Assessment)?

- A. Yes, but only if the biometric data is stored for more than five years.
- B. No, because DPIAs are only required when processing personal data on a large scale, which is not specified in this case.
- C. No, because explicit consent has already been obtained from the data subjects.
- **D. Yes, because biometric data is considered special category personal data, and its processing is likely to involve high risk.**

Answer: D

Explanation:

Under Article 35(3)(b) of GDPR, a DPIA is mandatory for processing that involves large-scale processing of special category data, including biometric data. Even if explicit consent is obtained, the risks associated with biometric processing require further evaluation.

- * Option A is correct because biometric data processing poses high risks to fundamental rights and freedoms, necessitating a DPIA.
- * Option B is incorrect because obtaining consent does not eliminate the requirement to conduct a DPIA.
- * Option C is incorrect because DPIAs are required for biometric processing regardless of scale if risks are present.
- * Option D is incorrect because storage 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 # 37

.....

Using GDPR exam prep is an important step for you to improve your soft power. I hope that you can spend a little time understanding what our study materials have to attract customers compared to other products in the industry. GDPR exam dumps have a higher pass rate than products in the same industry. If you want to pass GDPR Certification, then it is necessary to choose a product with a high pass rate. Our study materials guarantee the pass rate from professional knowledge, services, and flexible plan settings. According to user needs, GDPR exam prep provides everything possible to ensure their success.

GDPR Updated Dumps: <https://www.preppdf.com/PECB/GDPR-prepaway-exam-dumps.html>

Ken: On one side of the spectrum are tests that can be created prior GDPR Instant Access to implementation, Looking at the major attempts to nail down its definition gives us a good glimpse at our own centroid.

Definitely a person who passed GDPR Exam can gain qualification to enter this area or have opportunity to get promotion, "Time is Money" is really true in today's world.

Many industries need such excellent workers, Besides, GDPR they made three versions for your reference, the PDF, APP and Online software version.

- BTW, DOWNLOAD part of PrepPDF GDPR dumps from Cloud Storage: <https://drive.google.com/open?id=1InPtG3flePESoDWBmIiZHsiNjBw8L>