

Real PECB GDPR Exam Questions with Verified Answers



PECB GDPR PECB Certified Data Protection Officer

**Questions & Answers PDF
(Demo Version – Limited Content)**

For More Information – Visit link below:

<https://p2pexam.com/>

Visit us at: <https://p2pexam.com/gdpr>

2025 Latest CertkingdomPDF GDPR PDF Dumps and GDPR Exam Engine Free Share: <https://drive.google.com/open?id=1luA748b2wuNF7SqfAIXgVkeYk2UpC1hw>

It is important to cover PECB Certified Data Protection Officer (GDPR) exam topics and check if you need to practice them. If you are talking about the PECB GDPR certification exam, you need to practice and overcome mistakes. If you do not practice for it, chances are that you might get confused while appearing for the GDPR Exam. When you get the test study material, it comes with the PECB GDPR practice exams (desktop & web-based) to solve.

PECB GDPR Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">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 2	<ul style="list-style-type: none">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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Data protection concepts: General Data Protection Regulation (GDPR), and compliance measures

>> GDPR Reliable Exam Braindumps <<

GDPR Flexible Learning Mode, GDPR Latest Study Materials

It is widely accepted that where there is a will, there is a way; so to speak, a man who has a settled purpose will surely succeed. To obtain the GDPR certificate is a wonderful and rapid way to advance your position in your career. In order to reach this goal of passing the GDPR exam, you need more external assistance to help yourself. We have engaged in this career for more than ten years and with our GDPR Exam Questions, you will not only get aid to gain your dreaming GDPR certification, but also you can enjoy the first-class service online.

PECB Certified Data Protection Officer Sample Questions (Q21-Q26):

NEW QUESTION # 21

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:

Soin's DPO conducted an internal data protection audit. Is this acceptable?

- A. Yes, the DPO can conduct an internal data protection audit as part of monitoring compliance
- B. No, the role of the DPO is to only assist the company in conducting an internal data protection audit
- C. No, only the supervisory authority is responsible for conducting investigations in the form of internal data protection audits

Answer: A

Explanation:

Under GDPR Article 39(1)(b), the DPO is responsible for monitoring compliance with GDPR, including conducting internal audits. The DPO's role includes overseeing data protection policies, raising awareness, and ensuring adherence to regulations. The internal audit conducted by the DPO at Soin aligns with these responsibilities. However, while the DPO can conduct internal audits, the supervisory authority is responsible for external investigations and enforcement actions under GDPR Article 58.

NEW QUESTION # 22

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 can benefit 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:

Based on scenario 7, due to the attack, personal data of EduCCS' clients (such as names, email addresses, and phone numbers) were unlawfully accessed.

According to GDPR, when must EduCCS inform its clients about this personal data breach?

- A. Without undue delay.
- B. Only if a significant financial impact is detected.
- C. Within 24 hours.
- D. No later than 72 hours after becoming aware of it.

Answer: A

Explanation:

Under Article 34 of GDPR, when a breach poses a high risk to the rights and freedoms of individuals, controllers must notify affected data subjects without undue delay.

* Option A is correct because data subjects must be informed without undue delay if their rights are at risk.

* Option B is incorrect because the 72-hour rule applies to notifying the supervisory authority, not data subjects.

* Option C is incorrect because there is no strict 24-hour requirement under GDPR.

* Option D is incorrect because notification is based on the risk to individuals, not financial impact.

References:

* GDPR Article 34(1) (Obligation to notify data subjects without undue delay)

* Recital 86 (Timely breach notification to affected individuals)

NEW QUESTION # 23

Scenario 1:

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 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 the purpose limitation principle?

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

Answer: C

Explanation:

Under Article 5(1)(b) of GDPR, personal data must be collected for specific, explicit, and legitimate purposes and cannot be further processed in a manner incompatible with those purposes. Sharing medical data with an insurance company is a separate purpose and requires explicit consent or another lawful basis.

References:

* GDPR Article 5(1)(b) (Purpose limitation)

NEW QUESTION # 24

Question:

What is the role of the DPO in a DPIA?

- A. Record the DPIA outcomes.
- B. Conduct the DPI
- **C. Determine if a DPIA is necessary.**
- D. Approve the DPIA and ensure all risks are eliminated.

Answer: C

Explanation:

Under Article 39(1)(c) of GDPR, the DPO advises on the necessity of conducting a DPIA but does not conduct it themselves. The controller is responsible for carrying out the DPIA.

- * Option B is correct because the DPO must determine whether a DPIA is required and provide recommendations.
- * Option A is incorrect because conducting the DPIA is the responsibility of the controller, not the DPO.
- * Option C is incorrect because while the DPO can assist, DPIA documentation is the controller's duty.
- * Option D is incorrect because DPOs 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 # 25

Scenario:

A shop owner decided to install a video surveillance system to protect the property against theft. However, the cameras also capture a considerable part of the store next door.

Question:

Which statement below is correct in this case?

- A. This provision does not fall under GDPR requirements as it does not pose a high threat to the rights and freedoms of data subjects.
- **B. Controllers or processors of personal data under this provision fall under GDPR, since the cameras should capture only the premises of the shop owner who installed the cameras.**
- C. GDPR does not apply to personal data collected by surveillance cameras if used for security purposes.
- D. Controllers or processors that provide the means of processing personal data for such activities should operate under community privacy requirements.

Answer: B

Explanation:

Under Article 2 of GDPR, the regulation applies whenever personal data is processed by automated means, including CCTV footage that captures identifiable individuals.

* Option C is correct because GDPR applies when surveillance cameras capture public or third-party areas beyond the shop owner's premises.

* Option A is incorrect because community privacy requirements do not override GDPR.

* Option B is incorrect because GDPR applies even if the risk is low, as long as personal data (images of identifiable individuals) is processed.

* Option D is incorrect because GDPR applies to security cameras unless used solely for personal or household purposes (Recital 18).

References:

- * GDPR Article 2(1) (Material scope includes video surveillance)
- * Recital 18 (Household exemption does not apply to public monitoring)

NEW QUESTION # 26

.....

Our GDPR test prep embraces latest information, up-to-date knowledge and fresh ideas, encouraging the practice of thinking out of the box rather than treading the same old path following a beaten track. As the industry has been developing more rapidly, our GDPR exam dumps have to be updated at irregular intervals in case of keeping pace with changes. To give you a better learning environment, our experts have specialized in the technology with the system upgraded to offer you the latest GDPR Exam practices. And you can enjoy free updates of our GDPR learning prep for one year.

GDPR Flexible Learning Mode: <https://www.certkingdompdf.com/GDPR-latest-certkingdom-dumps.html>

- GDPR Exam VCE: PECB Certified Data Protection Officer - GDPR Pass Guide - GDPR Study Guide ☐ Simply search for ☐ GDPR ☐ for free download on \Rightarrow www.testkingpass.com \Leftarrow ☐ GDPR Valid Exam Guide
- Check out the demo of the real, 100 percent free PECB GDPR ☐ Search for ☐ GDPR ☐ and easily obtain a free download on (www.pdfvce.com) ☐ Exam GDPR Reviews
- GDPR Exam VCE: PECB Certified Data Protection Officer - GDPR Pass Guide - GDPR Study Guide ☐ ☒ www.pass4test.com ☐ ☒ is best website to obtain \Rightarrow GDPR ☐ for free download ☐ GDPR Reliable Test Book

- 2026 GDPR: PECB Certified Data Protection Officer –High-quality Reliable Exam Braindumps ☐ Go to website ✓
www.pdfvce.com ☐✓☐ open and search for ➡ GDPR ☐ to download for free ☐GDPR Reliable Test Book
- The Best GDPR Reliable Exam Braindumps - Leader in Certification Exams Materials - Fantastic GDPR Flexible Learning Mode ☐ Enter ☐ www.dumpsquestion.com ☐ and search for ☐ GDPR ☐ to download for free ☐Valid GDPR Learning Materials
- 2026 GDPR: Pass-Sure PECB Certified Data Protection Officer Reliable Exam Braindumps ☐ Open website ▶
www.pdfvce.com ◀ and search for [GDPR] for free download ☐Valid GDPR Test Guide
- 2026 GDPR: Pass-Sure PECB Certified Data Protection Officer Reliable Exam Braindumps ☐ The page for free
download of 【 GDPR 】 on ⇒ www.vce4dumps.com ⇐ will open immediately ☐Exam GDPR Reviews
- GDPR Practice Test Engine ☐ GDPR Practice Test Engine ☐ Valid GDPR Test Guide ☐ Download ☼ GDPR ☐☼☐
for free by simply entering ☐ www.pdfvce.com ☐ website ♣Valid GDPR Exam Vce
- Pass Guaranteed 2026 PECB Valid GDPR: PECB Certified Data Protection Officer Reliable Exam Braindumps ☐ Easily
obtain free download of 《 GDPR 》 by searching on （ www.easy4engine.com ） ☐GDPR Reliable Test Simulator
- GDPR Reliable Exam Vce ☐ Latest GDPR Examprep ☐ GDPR Practice Test Engine ☐ Simply search for ➡ GDPR ☐
☐ for free download on ⇒ www.pdfvce.com ⇐ ☐Valid GDPR Test Guide
- GDPR Reliable Exam Braindumps: PECB Certified Data Protection Officer - Latest PECB GDPR Flexible Learning Mode
☐ Download { GDPR } for free by simply searching on ➤ www.prepawaypdf.com ☐☐GDPR Verified Answers
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, 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, Disposable vapes

What's more, part of that CertkingdomPDF GDPR dumps now are free: <https://drive.google.com/open?id=1luA748b2wuNF7SqfAIXgVkeYk2UpC1hw>