GDPR Prüfungsguide: PECB Certified Data Protection Officer & GDPR echter Test & GDPR sicherlich-zu-bestehen

Übrigens, Sie können die vollständige Version der EchteFrage GDPR Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=1Zjjk1PsKFJ6fe8yHw_B9p7IqVAaSjQm4

Wollen Sie durch die PECB GDPR Zertifizierungsprüfung Ihre Position in der heutigen kunkurrenzfähigen IT-Branche und Ihre beruflichen Fähigkeiten verstärken? Dann müssen Sie mit breiten fachlichen Kenntnissen ausgerüstet sein. Und es ist nicht so einfach, die PECB GDPR Zertifizierungsprüfung zu bestehen. Vielleicht ist die PECB GDPR Zertifizierungsprüfung ein Sprungbrett, um im IT-Bereich befördert zu werden. Aber man braucht doch nicht, sich mit so viel Zeit und Energie für die Prüfung verwenden. Sie können unsere EchteFrage Produkte wählen, die speziellen Schulungsunterlagen für die IT-Zertifizierungsprüfungen bieten.

PECB GDPR Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Data protection concepts: General Data Protection Regulation (GDPR), and compliance measures
Thema 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.
Thema 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.
Thema 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 Exam <<

GDPR Zertifizierungsprüfung - GDPR Prüfungs-Guide

Ob Sie glauben oder nicht, bieten wir die autoritativen und wirkungsvollen Prüfungsunterlagen der PECB GDPR. Wir sind sehr bereit, die beste Hilfe der PECB GDPR Prüfungsvorbereitung Ihnen anzubieten. Vielleicht brauchen Sie nur die Zertifizierung der PECB GDPR, um Ihren Wunsch des Aufstiegs zu erfüllen. Wir wissen, dass man leicht den Impulskauf bereuen, deshalb empfehlen wir Ihnen, zuerst zu probieren und dann zu kaufen. Die Demo der Prüfungsunterlagen der PECB GDPR können Sie auf unserer Website einfach herunterladen. Probieren Sie mal!

PECB Certified Data Protection Officer GDPR Prüfungsfragen mit Lösungen (Q83-Q88):

83. Frage
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:
Scenario:
Soyled's customers are required to provide theirbank account detailsto buy a product. According to the GDPR, is this data processing lawful?

- A. No, sensitive data, such as bank account details, should only be processed by official authorities.
- B. Yes, because Soyled has a privacy policy in place that ensures the protection of personal data.
- C. Yes, because the processing is necessary for the fulfillment of the purchase agreement.
- D. No, because financial information cannot be collected without explicit consent.

Antwort: C

Begründung:
UnderArticle 6(1)(b) of GDPR, processing is lawfulif it is necessary for the performance of a contract with the data subject. Since the customers must provide bank details to complete their purchases, this processing isnecessaryfor fulfilling the agreement.
* Option A is correctbecause payment data is essential for transaction processing, which aligns with GDPR's contract basis.
* Option B is incorrectbecause having a privacy policy does not automatically justify data processing.
* Option C is incorrectbecause financial data can be processed byauthorized commercial entitiesunder GDPR.
* Option D is incorrectbecauseexplicit consent is not requiredwhen processing is contractually necessary.
References:
* GDPR Article 6(1)(b)(Processing necessary for contract performance)
* Recital 44(Necessity of processing for contract fulfillment)

84. Frage
Question:
What is therole of the European Data Protection Board (EDPB)?

- A. Tonegotiate and adopt EU lawsas per the proposals from the European Commission.

- B. Tosupervise and monitorthe application of GDPR within the EU.
- C. Toadvise the European Commissionregarding data protection issues in the EU.
- D. Toconduct audits on organizationssuspected of GDPR violations.

Antwort: C

Begründung:
UnderArticle 70 of GDPR, theEDPB is responsible for ensuring consistency in GDPR application and advising the European Commissionon data protection matters.
* Option B is correctbecausethe EDPB provides opinions and guidelines on GDPR implementation.
* Option A is incorrectbecausesupervision and enforcement are the responsibility of national supervisory authorities, not the EDPB.
* Option C is incorrectbecauseEU laws are adopted by the European Parliament and Council, not the EDPB.
* Option D is incorrectbecausethe EDPB does not conduct audits; national data protection authorities do.
References:
* GDPR Article 70(1)(b)(EDPB's advisory role)
* Recital 139(EDPB ensures consistency in GDPR application)

85. Frage
Question:
According to theprinciple of data minimization, data must be:

- A. Acquired only forspecified, explicit, and legitimate purposes.
- B. Adequate, relevant, and limitedto what is necessary in relation to the purposes of processing.
- C. Stored forno more than five yearsfrom the date of collection.
- D. In a formwhich permits the identification of data subjectsfor no longer than is necessary.

Antwort: B

Begründung:
UnderArticle 5(1)(c) of GDPR, data minimization requires thatpersonal data must be adequate, relevant, and limited to what is necessaryfor its intended purpose.
* Option C is correctbecause itdirectly reflects the GDPR's data minimization principle.
* Option A is incorrectbecausestorage limitation is a separate principle under Article 5(1)(e).
* Option B is incorrectbecausepurpose limitation (Article 5(1)(b)) is separate from data minimization.
* Option D is incorrectbecauseGDPR does not specify a fixed retention period (e.g., five years)- retention should be based on necessity.
References:
* GDPR Article 5(1)(c)(Data minimization principle)
* Recital 39(Controllers must collect only necessary data)

86. Frage
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 holderof 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 thepurpose limitation principle?

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

Antwort: A

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

Antwort: B

Begründung:
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)

88. Frage
.....