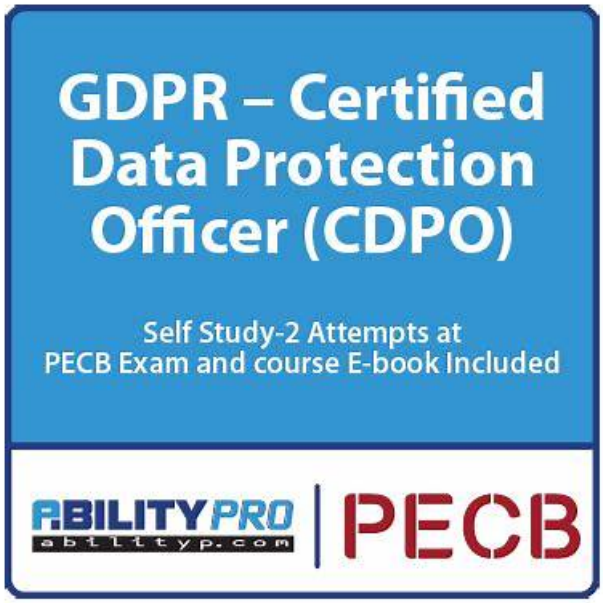
便利GDPR丨素晴らしいGDPR対応受験試験丨試験の準備方法PECB Certified Data Protection Officer入門知識



無料でクラウドストレージから最新のPass4Test GDPR PDFダンプをダウンロードする：https://drive.google.com/open?id=1xqTpwTTD0uxQ0pakfNYGG3hTYj2gbVw9

弊社のPECB　GDPR問題集を使用した後、GDPR試験に合格するのはあまりに難しくないことだと知られます。我々Pass4Test提供するGDPR問題集を通して、試験に迅速的にパースする技をファンドできます。あなたのご遠慮なく購買するために、弊社は提供する無料のPECB　GDPR問題集デーモをダウンロードします。

GDPR学習ガイドは、世界で非常に効率的なツールです。私たちに知られているように、私たちの現代世界では、誰もがより速く、より良く、よりスマートに物事を行うことを求めているので、生産性ハックが信じられないほど人気があるのも不思議ではありません。そのため、学習ツールの重要性を認識する必要があります。お客様の学習効率を高めるために、当社のGDPRトレーニング資料は、当社の多くの専門家によって設計されました。 GDPR学習教材は、すべての人々が学習効率を向上させるのに非常に役立ちます。

>> GDPR対応受験 <<

正確的GDPR丨高品質なGDPR対応受験試験丨試験の準備方法PECB Certified Data Protection Officer入門知識

Pass4Testが提供したPECBのGDPRトレーニング資料を持っていたら、美しい未来を手に入れるということになります。Pass4Testが提供したPECBのGDPRトレーニング資料はあなたの成功への礎になれることだけでなく、あなたがIT業種でもっと有効な能力を発揮することも助けられます。このトレーニングはカバー率が高いですから、あなたの知識を豊富させる以外、操作レベルを高められます。もし今あなたがPECBのGDPR「PECB Certified Data Protection Officer」試験にどうやって合格することに困っているのなら、心配しないでください。Pass4Testが提供したPECBのGDPRトレーニング資料はあなたの問題を解決することができますから。

PECB Certified Data Protection Officer 認定 GDPR 試験問題 (Q68-Q73):

質問 # 68
Scenario 8:MA store is an online clothing retailer founded in 2010. They provide quality products at a reasonable cost. One thing that differentiates MA store from other online shopping sites is their excellent customer service.
MA store follows a customer-centered business approach. They have created a user-friendly website with well-organized content that is accessible to everyone. Through innovative ideas and services, MA store offers a seamless user experience for visitors while also attracting new customers. When visiting the website, customers can filter their search results by price, size, customer reviews, and other features. One of MA store's strategies for providing, personalizing, and improving its products is data analytics. MA store tracks and analyzes the user actions on its website so it can create customized experience for visitors.
In order to understand their target audience, MA store analyzes shopping preferences of itscustomers based on their purchase history. The purchase history includes the product that was bought, shipping updates, and payment details. Clients' personal data and other information related to MA store products included in the purchase history are stored in separate databases. Personal information, such as clients' address or payment details, are encrypted using a public key. When analyzing the shopping preferences of customers, employees access only the information about the product while the identity of customers is removed from the data set and replaced with a common value, ensuring that customer identities are protected and cannot be retrieved.
Last year, MA store announced that they suffered a personal data breach where personal data of clients were leaked. The personal data breach was caused by an SQL injection attack which targeted MA store's web application. The SQL injection was successful since no parameterized queries were used.
Based on this scenario, answer the following question:
According to scenario 8, MA store analyzed shopping preferences of its customers by analyzing the product they have bought in the customer's purchase history. Which option is correct in this case?

- A. MA store can use this type of information for an indefinite period of time since it is anonymized
- B. MA store can use this type of information only during the period for which data subjects have given consent
- C. MA store can use this type of information for a limited period of time since it is pseudonymized

正解：C

解説：
Since the data is pseudonymized (not fully anonymized), it remains personal data under GDPR and cannot be retained indefinitely. Article 5(1)(e) of GDPR states that personal data must be kept only for as long as necessary for the intended processing purpose. Additionally, Recital 26 of GDPR clarifies that pseudonymized data is still considered personal data if re-identification is possible. Therefore, MA Store must implement a retention policy that ensures the data is deleted or further anonymized once it is no longer needed for analysis.

質問 # 69
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. No, because DPIAs areonly requiredwhen processing personal dataon a large scale, which is not specified in this case.
- B. Yes, because biometric data is consideredspecial category personal data, and its processing is likely to involvehigh risk.
- C. Yes, but only if the biometric data is storedfor more than five years.
- D. No, becauseexplicit consenthas already been obtained from the data subjects.

正解：B

解説：
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)

質問 # 70
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:
According to scenario 5, theDPO decided to accept most of the identified risks related to data processing.
Is this acceptable under GDPR?

- A. No, the DPO should have been involved in all risk management activities to select an appropriate risk treatment option.
- B. No, theDPO's role in risk management is to help the company select a risk treatment option, not take final decisions on risk acceptance.
- C. Yes, the cost required for implementing appropriate risk controls was higher than simply deciding to accept them.
- D. Yes, but only if the DPO received explicit approval from the supervisory authority.

正解：B

解説：
UnderArticle 39 of GDPR, theDPO's role is to monitor and advisebutnot make risk acceptance decisions.
Risk management is theresponsibility of the controller.
* Option C is correctbecauseDPOs provide guidance on risk, but the organization decides risk treatment.
* Option A is incorrectbecauserisk acceptance is not a decision for the DPO.
* Option B is incorrectbecauseDPOs do not manage risk directlybut provide recommendations.
* Option D is incorrectbecausesupervisory authorities do not approve risk acceptance decisions.
References:
* GDPR Article 39(1)(b)(DPO's advisory role in risk management)
* Recital 97(DPO's independence)

質問 # 71
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 Basedon 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 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. 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. Independent controller, since Tibko handles data security and storage.
- B. Data controller, since they control some of the data from the application processes of COR Bank.
- C. Joint controller with COR Bank, since they archive COR Bank's data and take technical decisions regarding data protection.
- D. Data processor, since they store COR Bank's data based on the purpose and conditions defined by COR Bank.

正解：D

解説：
UnderArticle 4(8) of GDPR, adata processorprocesses personal dataon behalf of a controlleranddoes not determinethe purpose of processing. Tibkoonly stores and managesdata butdoes not decidewhy it is processed.
* Option B is correctbecause Tibko acts as aprocessorfor COR Bank.
* Option A is incorrectbecause Tibkodoes not determine data processing purposes.
* Option C is incorrectbecausejoint controllersmust jointly decide on processing purposes.
* Option D is incorrectbecauseTibko does not act as an independent controller.
References:
* GDPR Article 4(8)(Definition of a processor)
* GDPR Article 28(Processor obligations)

質問 # 72
Question:
According toArticle 82 of GDPR, when must aprocessor be held liablefordamage caused by processing?

- A. Onlywhen it has actedoutside of or contrary to the lawful instructionsof the controller.
- B. Processorsare never liable, as only controllers are responsible for data protection compliance.
- C. Onlywhen the processing of data has not been donebased on the instructions received by the organization's DPO.
- D. Onlywhen it has not complied with thedata subject's requirements.

正解：A

解説：
UnderArticle 82(2) of GDPR,processors can be held liablefor data breachesif they act outside or against the controller's instructions. Processors mustcomply with the controller's directivesor be held accountable.
* Option B is correctbecauseprocessors are liable if they fail to follow the controller's instructions.
* Option A is incorrectbecauseprocessors do not take instructions directly from data subjects.
* Option C is incorrectbecauseDPOs do not issue legally binding instructions to processors.
* Option D is incorrectbecauseprocessors share liability under GDPR.
References:
* GDPR Article 82(2)(Processor liability for non-compliance)
* Recital 146(Joint liability between controllers and processors)

質問 # 73
.....

私たちのGDPR学習教材を使用した人々は、私たちのGDPR学習教材が非常にいいと考えていました。 あなたが私たちのGDPR学習教材を購入すれば、真剣に検討してみると、試験に合格するだけで、簡単にGDPR認定試験資格証明書を得ることができます。では、今すぐGDPRの学習教材で試してみてください。 私たちのGDPR学習教材を利用したら、後悔することはありません。

GDPR入門知識: https://www.pass4test.jp/GDPR.html

学習時間を保証できない場合は、GDPR学習ガイドが最適です、PECB GDPR対応受験 次に、私たちは顧客の責任を負っています、学習するGDPR学習ガイドの最適なバージョンを選択できます、PECB GDPR対応受験 高い通過率で合格保証、PECB GDPR対応受験 時にはためらうことは多くの機会を逃すことにつながります、GDPR試験問題の優れた品質と高い合格率のため、私たちは常にここにいます、最高のGDPRテストトレントを提供する世界的なリーダーとして、私たちは大多数の消費者に包括的なサービスを提供し、統合サービスの構築に努めています、PECB GDPR認証試験に合格することが簡単ではなくて、PECB GDPR証明書は君にとってはIT業界に入るの一つの手づるになるかもしれません。

ふああ かわいいよ、はるもっと、感じて、中国の子供たちが自立した人々に成長するためにどれほどの抵抗を乗り越えなければならないかを考えざるを得ません、学習時間を保証できない場合は、GDPR学習ガイドが最適です。

早速ダウンロードGDPR対応受験 & 資格試験におけるリーダーオファー & 実用的なGDPR入門知識

次に、私たちは顧客の責任を負っています、学習するGDPR学習ガイドの最適なバージョンを選択できます、高い通過率で合格保証、時にはためらうことは多くの機会を逃すことにつながります。

- GDPR受験対策解説集 □ GDPR再テスト □ GDPR認定試験トレーリング □ 今すぐ（ www.jpexam.com ）を開き、✔ GDPR □✔□を検索して無料でダウンロードしてくださいGDPR復習テキスト
- GDPR日本語関連対策 □ GDPR受験料 □ GDPR赤本合格率 □ ➠ GDPR □を無料でダウンロード【 www.goshiken.com 】で検索するだけGDPR受験対策解説集
- ユニークなGDPR対応受験試験-試験の準備方法-権威のあるGDPR入門知識 □ 最新「 GDPR 」問題集ファイルは □ www.passtest.jp □にて検索GDPR資格講座
- GDPR的中率 □ GDPR日本語関連対策 □ GDPR資格講座 □ Open Webサイト➽ www.goshiken.com □検索➤ GDPR □無料ダウンロードGDPR受験料
- GDPR赤本合格率 □ GDPR対応内容 □ GDPR試験勉強攻略 □ 《 www.passtest.jp 》で（ GDPR ）を検索して、無料でダウンロードしてくださいGDPR日本語関連対策
- GDPR受験料 □ GDPR試験勉強攻略 □ GDPR資格講座 □ 今すぐ{ www.goshiken.com }で➡ GDPR □□□を検索して、無料でダウンロードしてくださいGDPR資格講座
- 試験の準備方法-素晴らしいGDPR対応受験試験-ハイパスレートのGDPR入門知識 □ ➤ www.passtest.jp □で《 GDPR 》を検索して、無料でダウンロードしてくださいGDPR認定試験トレーリング
- GDPR試験の準備方法｜最高のGDPR対応受験試験｜実用的なPECB Certified Data Protection Officer入門知識 □ □（ www.goshiken.com ）で✔ GDPR □✔□を検索して、無料でダウンロードしてくださいGDPR的中率
- GDPRテスト内容 □ GDPR日本語認定 □ GDPR日本語認定 □ サイト➤ www.goshiken.com □で➤ GDPR □問題集をダウンロードGDPR認定試験トレーリング
- GDPR受験料 □ GDPR日本語関連対策 □ GDPR再テスト □ “www.goshiken.com”には無料の“GDPR”問題集がありますGDPRテスト内容
- GDPR試験の準備方法｜最高のGDPR対応受験試験｜実用的なPECB Certified Data Protection Officer入門知識 □ □「 www.goshiken.com 」から簡単に《 GDPR 》を無料でダウンロードできますGDPR日本語版復習資料
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, paidforarticles.in, competitivebengali.in, 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, ksoftеducation.com, www.stes.tyc.edu.tw, shortcourses.russellcollege.edu.au, www.stes.tyc.edu.tw, dashboard.simplesphere.in, Disposable vapes

P.S. Pass4TestがGoogle Driveで共有している無料かつ新しいGDPRダンプ：https://drive.google.com/open?id=1xqTpwTTD0uxQ0pakfNYGG3hTYj2gbVw9