信頼的CIPP-E｜最高のCIPP-E最新関連参考書試験｜試験の準備方法Certified Information Privacy Professional/Europe (CIPP/E) PDF問題サンプル

さらに、ShikenPASS CIPP-Eダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1HlhpPS4kz7UdLLeLVcON65lrY5TwF9_w

ShikenPASSは、このような効率的な学習計画を設計して、今後の開発のために効率の高い学習態度を構築できるようにすることを期待しています。私たちのCIPP-E研究急流は、あなたが学生や事務員、緑の手、または長年の経験のあるスタッフであっても、すべての候補者に対応します。したがって、CIPP-E試験に合格できるかどうかを心配する必要はありません。当社の技術力で成功することが保証されているからです。 CIPP-E試験問題の言語はわかりやすく、CIPP-E学習ガイドの合格率は99％～100％です。

IAPP CIPP-E認定試験は、ヨーロッパまたはヨーロッパのデータを使用しているプライバシーの専門家にとって貴重な資格です。この試験は、GDPRおよびデータ保護原則に関する候補者の知識をテストするように設計されており、世界最大のプライバシー専門家協会によって提供されています。認定は3年間有効であり、継続教育クレジットを獲得することで更新できます。

>> CIPP-E最新関連参考書 <<

コンプリートCIPP-E最新関連参考書 & 資格試験のリーダー & 最新のCIPP-E PDF問題サンプル

クライアントがCIPP-Eクイズ準備を購入する前後に、思いやりのあるオンラインカスタマーサービスを提供します。クライアントは、購入前にCIPP-E試験実践ガイドの価格、バージョン、内容を尋ねることができます。ソフトウェアの使用方法、CIPP-Eクイズ準備の機能、CIPP-E学習資料の使用中に発生する問題、および払い戻しの問題について相談できます。オンラインカスタマーサービスの担当者がCIPP-E試験実践ガイドに関する質問に回答し、辛抱強く情熱的に問題を解決します。

CIPP/E認定は、データ保護担当者、プライバシーコンサルタント、プライバシー法律家、プライバシーオーディターなど、プライバシー関連の業務に携わる個人に適しています。また、組織内でデータ保護ポリシーや手順を管理･実装する責任を持つ個人にも適しています。CIPP/E認定は、欧州のデータ保護法や規制に準拠して組織が運営されることを保証するための必要な知識とスキルを提供します。

IAPP Certified Information Privacy Professional/Europe (CIPP/E) 認定 CIPP-E 試験問題 (Q262-Q267):

質問 # 262
In which of the following cases would an organization MOST LIKELY be required to follow both ePrivacy and data protection rules?

- A. When paying a search engine company to give prominence to certain products and services within specific search results.
- B. When creating an untargeted pop-up ad on a website.
- C. When emailing a customer to announce that his recent order should arrive earlier than expected.
- D. When calling a potential customer to notify her of an upcoming product sale.

正解：A

解説：
The ePrivacy Directive (ePD) and the General Data Protection Regulation (GDPR) are two EU laws that regulate different aspects of personal data processing. The ePD focuses on electronic communications and the use of cookies and similar technologies, while the GDPR covers the broader principles and rights of data protection. Both laws apply to any organization that processes personal data of individuals in the EU, regardless of where the organization is located.
Option D involves both electronic communication and personal data processing, and therefore requires compliance with both ePD and GDPR. Paying a search engine company to give prominence to certain products and services within specific search results implies the use of cookies or similar technologies to track the online behavior of users and target them with personalized ads. This requires the consent of the users under the ePD, as well as the provision of clear and comprehensive information about the purpose and scope of the data processing. Moreover, the organization must comply with the GDPR requirements for data protection by design and by default, data minimization, data security, data subject rights, and accountability.
Option A only involves the use of cookies or similar technologies, and therefore only requires compliance with the ePD. Creating an untargeted pop-up ad on a website does not involve the processing of personal data, as the ad is not based on the online behavior or preferences of the users. However, the organization must still obtain the consent of the users for the use of cookies or similar technologies, and provide them with clear and comprehensive information about the purpose and scope of the data processing.
Option B only involves the processing of personal data, and therefore only requires compliance with the GDPR. Calling a potential customer to notify her of an upcoming product sale involves the collection and use of the customer's personal data, such as name, phone number, and purchase history. The organization must have a lawful basis for the data processing, such as consent, contract, or legitimate interest, and must respect the data subject rights, such as the right to object, the right to access, and the right to erasure.
Option C only involves the processing of personal data, and therefore only requires compliance with the GDPR. Emailing a customer to announce that his recent order should arrive earlier than expected involves the use of the customer's personal data, such as name, email address, and order details. The organization must have a lawful basis for the data processing, such as consent, contract, or legitimate interest, and must respect the data subject rights, such as the right to object, the right to access, and the right to erasure.
Reference:
Free CIPP/E Study Guide, page 15, section 2.3.3
CIPP/E Certification, page 10, section 1.1.2
Cipp-e Study guides, Class notes & Summaries, document "CIPP/E Exam Summary 2023", page 42, section 2.3.3 ePrivacy: The EU's other data protection rule The New Rules of Data Privacy A guide to GDPR data privacy requirements A guide to the data protection principles

質問 # 263
According to the European Data Protection Board, if a controller that is not established in the EU but still subject to the GDPR becomes aware of a personal data breach, which supervisory authority or authorities must be notified?

- A. Only the supervisory authority of the EU member state in which the controller's EU representative (pursuant to Article 27) is established.
- B. Only one lead supervisory authority, as a controller benefits from the one-stop shop mechanism under the GDPR's enforcement regime.
- C. Every supervisory authority of the EU member states where the controller is offering goods or services.
- D. Every supervisory authority for which affected data subjects reside in their EU member state.

正解：A

解説：
The General Data Protection Regulation (GDPR) introduces a duty for controllers to notify the competent supervisory authority of a personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The GDPR also requires controllers to communicate the personal data breach to the affected data subjects without undue delay, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services to data subjects in the EU or the monitoring of their behaviour as far as their behaviour takes place within the EU.
The GDPR provides that where a controller or a processor is not established in the EU, but is subject to the GDPR, the controller or the processor shall designate in writing a representative in the EU. The representative shall be established in one of the member states where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are. The representative shall act on behalf of the controller or the processor and may be addressed by any supervisory authority or data subject on any issues related to the processing of personal data under the GDPR.
The GDPR also establishes a one-stop shop mechanism, which aims to ensure the consistent and effective application of the GDPR across the EU. The one-stop shop mechanism allows a controller or a processor with establishments in several member states to have a single supervisory authority as its interlocutor, which is the supervisory authority of the main establishment or of the single establishment of the controller or processor.
The one-stop shop mechanism also enables a controller or a processor that is not established in the EU, but is subject to the GDPR, to deal with a single lead supervisory authority, which is the supervisory authority of the member state where the representative of the controller or processor is established.
Based on the GDPR and the guidelines of the European Data Protection Board (EDPB), if a controller that is not established in the EU but still subject to the GDPR becomes aware of a personal data breach, the controller must notify the supervisory authority of the EU member state in which the controller's EU representative (pursuant to Article 27) is established. This is the only supervisory authority that the controller must notify, as the controller benefits from the one-stop shop mechanism and has a single lead supervisory authority. The controller does not need to notify every supervisory authority of the EU member states where the controller is offering goods or services or where the affected data subjects reside, as this would be contrary to the principle of consistency and the aim of simplification of the one-stop shop mechanism.
References:
GDPR, Articles 3, 4, 27, 28, 29, 33, 34, 51, 55, 56, 57, 58, 60, 61, 62, 63, 64, 65, 66, 67, and 68.
EDPB Guidelines 9/2022 on personal data breach notification under GDPR, pages 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, and 16.
EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, pages 19, 20, 21, 22, 23, 24, 25, 26, 27, and 28.
EDPB Guidelines 3/2018 on the territorial scope of the GDPR, pages 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, and 15.

質問 # 264
Which of the following would MOST likely trigger the extraterritorial effect of the GDPR, as specified by Article 3?

- A. The behavior of suspected terrorists being monitored by EU law enforcement bodies.
- B. The behavior of EU citizens outside the EU being monitored by non-EU law enforcement bodies.
- C. Personal data of EU citizens being processed by a controller or processor based outside the EU.
- D. Personal data of EU residents being processed by a non-EU business that targets EU customers.

正解：C

解説：
Explanation/Reference: https://hsfnotes.com/data/2019/12/02/edpb-adopts-final-guidelines-on-gdpr-extra-territoriality/

質問 # 265
SCENARIO
Please use the following to answer the next question:
ProStorage is a multinational cloud storage provider headquartered in the Netherlands. Its CEO. Ruth Brown, has developed a two-pronged strategy for growth: 1) expand ProStorage s global customer base and 2) increase ProStorage's sales force by efficiently onboarding effective teams. Enacting this strategy has recently been complicated by Ruth's health condition, which has limited her working hours, as well as her ability to travel to meet potential customers. ProStorage's Human Resources department and Ruth's Chief of Staff now work together to manage her schedule and ensure that she is able to make all her medical appointments The latter has become especially crucial after Ruth's last trip to India, where she suffered a medical emergency and was hospitalized m New Delhi Unable to reach Ruths family, the hospital reached out to ProStorage and was able to connect with her Chief of Staff, who in coordination with Mary, the head of HR. provided information to the doctors based on accommodate on requests Ruth made when she started a: ProStorage What transfer mechanism did ProStorage most likely rely on to transfer Ruth's medical information to the

hospital?

- A. Protecting against legal liability from Ruth.
- B. Performance of a contract with Ruth.
- C. Ruth's implied consent.
- D. Protecting the vital interest of Ruth

正解：A

質問 # 266
How does the GDPR now define "processing"?

- A. Any operation or set of operations performed on personal data or on sets of personal data.
- B. Any act involving the collecting and recording of personal data.
- C. Any use or disclosure of personal data compatible with the purpose for which the data was collected.
- D. Any operation or set of operations performed by automated means on personal data or on sets of personal data.

正解：A

解説：
Reference https://gdpr-info.eu/issues/processing/

質問 # 267
.....

id=1HlhpPS4kz7UdLLeLVcON65lrY5TwF9_w