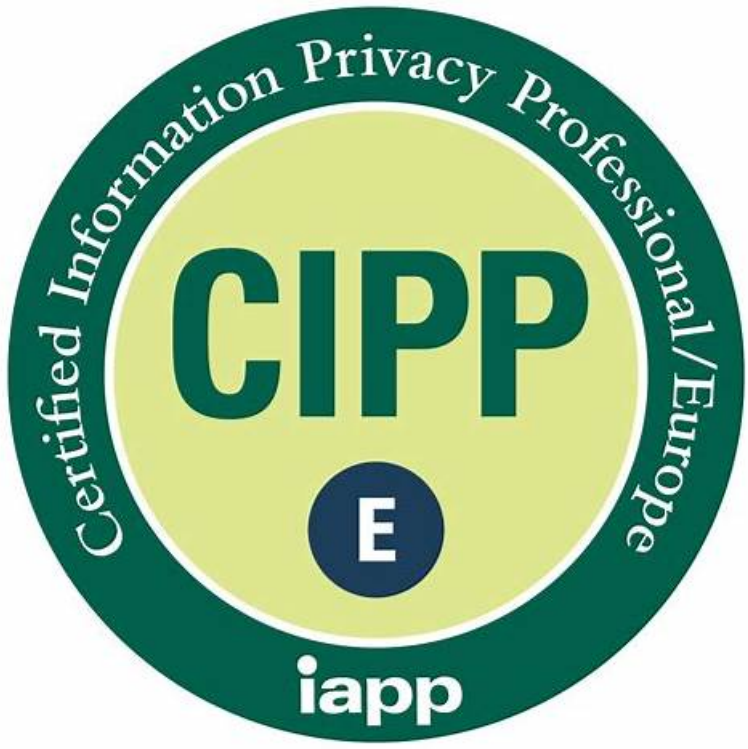
Pass Guaranteed Quiz CIPP-E - Certified Information Privacy Professional/Europe (CIPP/E)–Professional Exam Online



P.S. Free 2026 IAPP CIPP-E dumps are available on Google Drive shared by DumpExam: https://drive.google.com/open?id=1iW15Q0XHG0FT2wStZCQIIiL3luvZJxBW

Certified Information Privacy Professional/Europe (CIPP/E) CIPP-E practice test not only gives you the opportunity to practice with real exam questions but also provides you with a self-assessment report highlighting your performance in an attempt. DumpExam keeps an eye on changes in the IAPP CIPP-E exam syllabus and updates Certified Information Privacy Professional/Europe (CIPP/E) CIPP-E Exam Dumps accordingly to make sure they are relevant to the latest exam topics. After making the payment for Certified Information Privacy Professional/Europe (CIPP/E) CIPP-E dumps questions you'll be able to get free updates for up to 365 days.

The CIPP-E certification exam is designed for professionals who are involved in privacy-related roles such as data protection officers, privacy consultants, privacy lawyers, compliance officers, and information security professionals. CIPP-E exam is also ideal for professionals who are looking to advance their careers in the privacy field or those who are new to the field and are looking to gain a comprehensive understanding of the privacy laws and regulations of Europe.

Target Audience

The complete form of the CIPP-E is the Certified Information Privacy Professional/Europe. The exam, in particular, is designed for data protection officers who are responsible for keeping tabs on compliance, being in charge of internal data security, training staff for data processing, and auditing. However, such a test is more specific on trans-border data protection officials.

>> CIPP-E Exam Online <<

Certified Information Privacy Professional/Europe (CIPP/E) pass4sure practice & CIPP-E pdf training material

Our company is a professional certificate exam materials provider, we have occupied in this field for years, and we have rich

experiences. CIPP-E exam cram is edited by professional experts, and they are quite familiar with the exam center, and therefore, the quality can be guaranteed. In addition, CIPP-E training materials contain both questions and answers, and it also has certain quantity, and it's enough for you to pass the exam. In order to strengthen your confidence for CIPP-E Training Materials , we are pass guarantee and money back guarantee, if you fail to pass the exam we will give you full refund, and no other questions will be asked.

The CIPP/E certification is ideal for individuals who work in privacy roles, including data protection officers, privacy consultants, privacy lawyers, and privacy auditors. Certified Information Privacy Professional/Europe (CIPP/E) certification is also suitable for individuals who are responsible for managing and implementing data protection policies and procedures in their organizations. The CIPP/E certification provides the necessary knowledge and skills to ensure that organizations comply with European data protection laws and regulations.

IAPP Certified Information Privacy Professional/Europe (CIPP/E) Sample Questions (Q238-Q243):

NEW QUESTION # 238
SCENARIO
Please use the following to answer the next question:
Sandy recently joined Market4U, an advertising technology company founded in 2016, as their VP of Privacy and Data Governance. Through her first initiative in conducting a data inventory, Sandy learned that Market4U maintains a list of 19 million global contacts that were collected throughout the course of Market4U's existence. Knowing the risk of having such a large amount of data, Sandy wanted to purge all contacts that were entered into Market4U's systems prior to May 2018, unless such contacts had a more recent interaction with Market4U content. However, Dan, the VP of Sales, informed Sandy that all of the contacts provide useful information regarding successful marketing campaigns and trends in industry verticals for Market4U's clients.
Dan also informed Sandy that he had wanted to focus on gaining more customers within the sports and entertainment industry. To assist with this behavior, Market4U's marketing team decided to add several new fields to Market4U's website forms, including forms for downloading white papers, creating accounts to participate in Market4U's forum, and attending events. Such fields include birth date and salary.
What should Sandy give as feedback to Dan and the marketing team regarding the new fields Dan wants to add to Market4U's forms?

- A. Make all the fields optional.
- B. Eliminate the fields as they are not necessary for the purposes of providing white papers or registration for events.
- C. Eliminate the fields, as they are not proportional to the services being offered.
- D. Only request the information in brackets (i.e., age group and salary range).

Answer: B

NEW QUESTION # 239
Which of the following entities would most likely be exempt from complying with the GDPR?

- A. A company that stores all customer data in Australia and is headquartered in a European Union (EU) member state.
- B. A South American company that regularly collects European customers' personal data.
- C. A Chinese company that has opened a satellite office in a European Union (EU) member state to service European customers.
- D. A North American company servicing customers in South Africa that uses a cloud storage system made by a European company.

Answer: D

Explanation:
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 (Article 3(1)). The GDPR also applies to the processing of personal data of data subjects who are in the EU by a controller or a processor not established in the EU, where the processing activities are related to the offering of goods or services to such data subjects in the EU, or the monitoring of their behaviour as far as their behaviour takes place within the EU (Article 3(2)). Therefore, the GDPR would apply to the following entities:
A South American company that regularly collects European customers' personal data, as it is offering goods or services to data subjects in the EU.
A company that stores all customer data in Australia and is headquartered in a European Union (EU) member state, as it has an

establishment in the EU.
A Chinese company that has opened a satellite office in a European Union (EU) member state to service European customers, as it has an establishment in the EU and is offering goods or services to data subjects in the EU.
The GDPR would not apply to the following entity:
A North American company servicing customers in South Africa that uses a cloud storage system made by a European company, as it does not have an establishment in the EU, nor is it offering goods or services to data subjects in the EU, nor is it monitoring their behaviour within the EU. The fact that it uses a cloud storage system made by a European company does not trigger the application of the GDPR, unless the cloud provider is also processing personal data on behalf of the North American company in the context of its activities in the EU.

NEW QUESTION # 240
Which of the following is NOT an explicit right granted to data subjects under the GDPR?

- A. The right to request access to the personal data a controller holds about them.
- B. The right to request restriction of processing of personal data, under certain scenarios.
- C. The right to opt-out of the sale of their personal data to third parties.
- D. The right to request the deletion of data a controller holds about them.

Answer: A

NEW QUESTION # 241
When is data sharing agreement MOST likely to be needed?

- A. When personal data is being shared with a public authority with powers to require the personal data to be disclosed.
- B. When personal data is being proactively shared by a controller to support a police investigation.
- C. When anonymized data is being shared.
- D. When personal data is being shared between commercial organizations acting as joint data controllers.

Answer: D

Explanation:
A data sharing agreement is a contract that documents what data is being shared and how it can be used. It can be used to make data sharing lawful and to demonstrate compliance with the accountability principle under the GDPR. A data sharing agreement is most likely to be needed when personal data is being shared between commercial organizations acting as joint data controllers, because they have to determine and agree on their respective roles and responsibilities, such as the purpose and legal basis of the data sharing, the rights of the data subjects, the security measures, and the liability for any breaches. A data sharing agreement is not mandatory, but it is good practice and can help to avoid disputes and confusion. A data sharing agreement may not be needed or may be less detailed in the other scenarios, depending on the circumstances and the nature of the data. For example, anonymized data is not personal data under the GDPR and does not require a data sharing agreement, although it may still be subject to other contractual or ethical obligations. Personal data that is proactively shared by a controller to support a police investigation may be covered by a legal obligation or a public interest, and the controller may not have much control over how the data is used by the police. Personal data that is shared with a public authority with powers to require the personal data to be disclosed may also be subject to a legal obligation or a public interest, and the controller may have to comply with the authority's request without a data sharing agreement. Reference:
Data sharing agreements | ICO, which provides guidance on the benefits and contents of a data sharing agreement.
Data Sharing Agreement - the Definition - GDPR Summary, which explains what a data sharing agreement is and when it can be used.
The role of data sharing and the GDPR | Data Republic, which discusses the impact of the GDPR on data sharing practices.

NEW QUESTION # 242
Once an organization has conducted an internal investigation to determine the scope of a ransomware attack, what is the appropriate next step in the process?

- A. Assess the risks associated with the breach and, if necessary, notify affected individuals and regulatory bodies within the relevant timeframes.
- B. Inform all customers and the public via social media platforms to ensure rapid dissemination of relevant information.
- C. Wait for law enforcement to provide guidance on notification procedures before taking any further action.

- D. Notify law enforcement and consult with legal counsel to understand the implications of the breach and the notification requirements.

Answer: A

Explanation:
The GDPR (General Data Protection Regulation) has strict data breach response requirements, particularly for ransomware attacks that affect personal data. The appropriate next step after an internal investigation is to assess the risks associated with the breach and notify affected parties if necessary.
Key GDPR Breach Response Steps (Article 33 & 34):
* Assess the risks to personal data
* If the breach poses a risk to individuals' rights and freedoms, the supervisory authority (DPA) must be notified within 72 hours.
* If there is a high risk, affected individuals must also be informed without undue delay.
* Why Answer Choice A is Correct
* Risk assessment is a critical first step after an internal investigation.
* If the breach meets the risk threshold, notification to authorities and individuals is required under GDPR.
* Why Other Answer Choices Are Incorrect:
* B (Notify Law Enforcement First): While law enforcement may be involved, GDPR does not mandate consulting law enforcement before conducting a risk assessment or notifying individuals.
* C (Informing the Public Immediately): Public disclosure via social media is not a GDPR requirement. Affected individuals and DPAs should be formally notified first.
* D (Waiting for Law Enforcement): GDPR does not allow waiting for law enforcement before fulfilling notification obligations. Controllers must act within 72 hours.
Conclusion: The correct next step after an internal investigation is to assess the risks and, if necessary, notify affected individuals and regulatory bodies as required under GDPR Articles 33 and 34.

NEW QUESTION # 243
.....

What's more, part of that DumpExam CIPP-E dumps now are free: https://drive.google.com/open?id=1iW15Q0XHG0FT2wStZCQIIiL3luvZJxBW