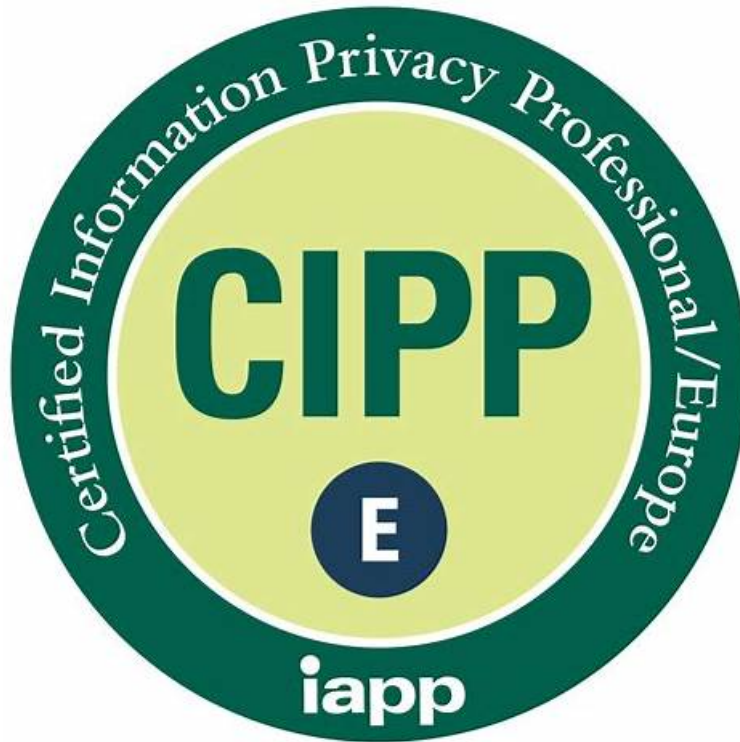


Pass Guaranteed Perfect CIPP-E - Certified Information Privacy Professional/Europe (CIPP/E) Valid Cram Materials



2026 Latest TestkingPDF CIPP-E PDF Dumps and CIPP-E Exam Engine Free Share: <https://drive.google.com/open?id=1iHWpLeBwGLoIn7b7QvwdE4FJoC0dDqnE>

our CIPP-E study materials will also save your time and energy in well-targeted learning as we are going to make everything done in order that you can stay focused in learning our CIPP-E study materials without worries behind. We are so honored and pleased to be able to read our detailed introduction and we will try our best to enable you a better understanding of our CIPP-E Study Materials better.

You may know that we are so popular for the passing rate of our CIPP-E guide quiz is very high. Generally speaking, 98 % - 99 % of the users can successfully pass the CIPP-E exam, obtaining the corresponding certificate. In addition, the content of our CIPP-E Exam Materials is easy to learn and suitable for the public. No matter what your previous learning level is, there will be no problem of understanding.

>> CIPP-E Valid Cram Materials <<

100% Pass IAPP - CIPP-E –High Pass-Rate Valid Cram Materials

TestkingPDF are supposed to help you pass the exam smoothly. Don't worry about channels to the best CIPP-E study materials because we are the exactly best vendor in this field for more than ten years. And so many exam candidates admire our generosity of the CIPP-E Practice Questions offering help for them. Up to now, no one has ever challenged our leading position of this area. With our CIPP-E training guide, you will be doomed to pass the exam successfully.

IAPP Certified Information Privacy Professional/Europe (CIPP/E) Sample Questions (Q176-Q181):

NEW QUESTION # 176
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 is the best way that Sandy can gain the insights that Dan seeks while still minimizing risks for Market4U?

- A. Conduct analysis only on pseudonymized personal data.
- B. Procure a third party to conduct the analysis and delete the data from Market4U's systems.
- **C. Conduct analysis only on anonymized personal data.**
- D. Delete all data collected prior to May 2018 after conducting the trend analysis.

Answer: C

NEW QUESTION # 177

Rental Market Champions (RMC) is a real estate agency, providing residential property rental services across Croatia. RMC processes personal data on their tenants, including names, contact details, employment data, financial information, credit scores and executed tenancy agreements.

RMC receives notification from a cybersecurity firm that RMC tenants' personal data have been posted to the dark web by a threat actor. Subsequent investigation by RMC confirms that their systems have been compromised and that sample files released on the dark web by the threat actor do relate to RMC customers.

RMC should notify the relevant supervisory authority of the data breach no later than 72 hours from which of the following actions?

- A. After receiving notification from the cybersecurity firm.
- B. After collating the information needed to notify the relevant supervisory authority.
- **C. After determining that the data breach is likely to result in a risk to the rights and freedoms of customers.**
- D. After establishing that customers' personal data have been compromised.

Answer: C

Explanation:

Under Article 33 GDPR, a controller must notify the supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it," unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The EDPB Guidelines 9/2022 on personal data breach notification clarify that "awareness" occurs when the controller has a reasonable degree of certainty that a security incident has led to personal data being compromised, and it has assessed that the breach is likely to result in risk.

Thus, the 72-hour clock starts not when first informed (D) or when data compromise is suspected (C), but once the controller determines that the breach is likely to pose risks to affected individuals. Collating additional details (B) may continue after notification, but cannot delay the notification itself.

#Reference:

* GDPR, Article 33(1)

* EDPB Guidelines 9/2022, Section II.A "When to notify"

* CIPP/E Textbook (3rd ed.), Chapter 10 "Security of Personal Data" (breach notification obligations)

NEW QUESTION # 178

Assuming that the "without undue delay" provision is followed, what is the time limit for complying with a data access request?

- A. Within 40 days of receipt
- **B. Within one month of receipt, which may be extended by up to an additional month**
- C. Within one month of receipt, which may be extended by an additional two months
- D. Within 40 days of receipt, which may be extended by up to 40 additional days

Answer: B

NEW QUESTION # 179

SCENARIO

Please use the following to answer the next question:

Due to rapidly expanding workforce, Company A has decided to outsource its payroll function to Company B.

Company B is an established payroll service provider with a sizable client base and a solid reputation in the industry.

Company B's payroll solution for Company A relies on the collection of time and attendance data obtained via a biometric entry system installed in each of Company A's factories. Company B won't hold any biometric data itself, but the related data will be uploaded to Company B's UK servers and used to provide the payroll service. Company B's live systems will contain the following information for each of Company A's employees:

- * Name
- * Address
- * Date of Birth
- * Payroll number
- * National Insurance number
- * Sick pay entitlement
- * Maternity/paternity pay entitlement
- * Holiday entitlement
- * Pension and benefits contributions
- * Trade union contributions

Jenny is the compliance officer at Company A. She first considers whether Company A needs to carry out a data protection impact assessment in relation to the new time and attendance system, but isn't sure whether or not this is required.

Jenny does know, however, that under the GDPR there must be a formal written agreement requiring Company B to use the time and attendance data only for the purpose of providing the payroll service, and to apply appropriate technical and organizational security measures for safeguarding the data. Jenny suggests that Company B obtain advice from its data protection officer. The company doesn't have a DPO but agrees, in the interest of finalizing the contract, to sign up for the provisions in full. Company A enters into the contract.

Weeks later, while still under contract with Company A, Company B embarks upon a separate project meant to enhance the functionality of its payroll service, and engages Company C to help. Company C agrees to extract all personal data from Company B's live systems in order to create a new database for Company B.

This database will be stored in a test environment hosted on Company C's U.S. server. The two companies agree not to include any data processing provisions in their services agreement, as data is only being used for IT testing purposes.

Unfortunately, Company C's U.S. server is only protected by an outdated IT security system, and suffers a cyber security incident soon after Company C begins work on the project. As a result, data relating to Company A's employees is visible to anyone visiting Company C's website. Company A is unaware of this until Jenny receives a letter from the supervisory authority in connection with the investigation that ensues.

As soon as Jenny is made aware of the breach, she notifies all affected employees.

Under the GDPR, which of Company B's actions would NOT be likely to trigger a potential enforcement action?

- A. Their omission of data protection provisions in their contract with Company C.
- B. Their failure to provide sufficient security safeguards to Company A's data.
- C. Their decision to operate without a data protection officer.
- **D. Their engagement of Company C to improve their payroll service.**

Answer: D

Explanation:

While Company B made several mistakes in handling Company A's employee data, not all of them would likely trigger a potential enforcement action under the GDPR. Here's an analysis of each option:

A: Omission of data protection provisions in the contract with Company C: This is a clear violation of the GDPR. Company B, as the data controller, is responsible for ensuring that any third-party processors comply with data protection requirements. By omitting data protection provisions in the contract, Company B failed to take appropriate steps to ensure the security and privacy of the personal data. This would be a likely trigger for an enforcement action.

B: Failure to provide sufficient security safeguards to Company A's data: This is another violation of the GDPR. Company B has a legal obligation to implement appropriate technical and organizational security measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction. The outdated IT security system at Company C's U.S. server demonstrates a failure to meet this obligation. This would also be a likely trigger for an enforcement action.

C: Engagement of Company C to improve their payroll service: While outsourcing certain aspects of data processing is permitted under the GDPR, the data controller remains ultimately responsible for compliance.

However, simply engaging another company to improve a service itself isn't necessarily a violation. As long as the proper safeguards are in place and the data processing is carried out in accordance with the GDPR, this action alone would not likely trigger an

enforcement action.

D: Decision to operate without a data protection officer: The GDPR requires certain organizations to appoint a data protection officer (DPO). While Company B may be required to have a DPO depending on its size and activities, the absence of a DPO wouldn't automatically trigger an enforcement action. However, it could indicate a lack of compliance culture and contribute to other violations, increasing the likelihood of an enforcement action.

Therefore, while Company B made several mistakes, only the ones that directly violate specific data protection requirements, such as omitting data protection provisions in contracts or failing to implement appropriate security measures, are likely to trigger an enforcement action. Engaging a third-party to improve a service, as long as it's done in a compliant manner, isn't a violation in itself.

NEW QUESTION # 180

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 in New Delhi. Unable to reach Ruth's 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 at ProStorage. In support of Ruth's strategic goals of hiring more sales representatives, the Human Resources team is focused on improving its processes to ensure that new employees are sourced, interviewed, hired, and onboarded efficiently. To help with this, Mary identified two vendors, HRYourWay, a German based company, and InstaHR, an Australian based company. She decided to have both vendors go through ProStorage's vendor risk review process so she can work with Ruth to make the final decision. As part of the review process, Jackie, who is responsible for maintaining ProStorage's privacy program (including maintaining controller BCRs and conducting vendor risk assessments), reviewed both vendors but completed a transfer impact assessment only for InstaHR. After her review of both boasted a more established privacy program and provided third-party attestations, whereas HRYourWay was a small vendor with minimal data protection operations.

Thus, she recommended InstaHR.

ProStorage's marketing team also worked to meet the strategic goals of the company by focusing on industries where it needed to grow its market share. To help with this, the team selected as a partner UpFinance, a US based company with deep connections to financial industry customers. During ProStorage's diligence process, Jackie from the privacy team noted in the transfer impact assessment that UpFinance implements several data protection measures including end-to-end encryption, with encryption keys held by the customer.

Notably, UpFinance has not received any government requests in its 7 years of business. Still, Jackie recommended that the contract require UpFinance to notify ProStorage if it receives a government request for personal data UpFinance processes on its behalf prior to disclosing such data.

Why is the additional measure recommended by Jackie sufficient for using UpFinance?

- A. UpFinance implements sufficient data protection measures
- B. UpFinance is in a highly regulated financial industry
- C. UpFinance is based in a country without surveillance laws.
- D. UpFinance is an established 7-year-old business.

Answer: A

Explanation:

According to Article 46 of the GDPR, in the absence of an adequacy decision by the European Commission, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. One of the possible appropriate safeguards is the use of standard data protection clauses adopted by the Commission or by a supervisory authority. However, Article 46(5) states that the possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority shall not affect the possibility for the controller or processor to rely upon other appropriate safeguards provided for in paragraph 2 of this Article, provided that they ensure that data subjects have enforceable and effective rights as regards the processing of their data. Therefore, in this case, Jackie's recommendation of requiring UpFinance to notify ProStorage if it receives a government request for personal data UpFinance processes on its behalf prior to disclosing such data is an additional measure that could be considered as an appropriate safeguard, especially since UpFinance implements several data protection measures, including end-to-end encryption, with encryption keys held by the customer, which would ensure a high level of security and confidentiality of the personal data transferred. Reference:

Article 46 of the GDPR

- [illegible]

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, 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,
www.stes.tyc.edu.tw, lms.col1920.co.uk, www.stes.tyc.edu.tw, legal.academiadeamparoindirecto.com, Disposable vapes

P.S. Free 2026 IAPP CIPP-E dumps are available on Google Drive shared by TestkingPDF: <https://drive.google.com/open?id=1iHWpLeBwGLoIn7b7QvwdE4FJoC0dDqnE>