



CIPP-E^{Q&As}

Certified Information Privacy Professional/Europe (CIPP/E)





Pass IAPP CIPP-E Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/cipp-e.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Which of the following describes a mandatory requirement for a group of undertakings that wants to appoint a single data protection officer?

- A. The group of undertakings must obtain approval from a supervisory authority.
- B. The group of undertakings must be comprised of organizations of similar sizes and functions.
- C. The data protection officer must be located in the country where the data controller has its main establishment.
- D. The data protection officer must be easily accessible from each establishment where the undertakings are located.

Correct Answer: D

Reference: <https://www.privacy-regulation.eu/en/article-37-designation-of-the-data-protection-officer-GDPR.htm>

QUESTION 2

SCENARIO

Please use the following to answer the next question: Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no

longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.

Since these measures would potentially impact employees, Building Block's Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.

After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees' computers activity and their location. During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization. The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased.

Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company's computers, and from working remotely without authorization.

To comply with the GDPR, what should Building Block have done as a first step before implementing the SecurityScan measure?

- A. Assessed potential privacy risks by conducting a data protection impact assessment.
- B. Consulted with the relevant data protection authority about potential privacy violations.



- C. Distributed a more comprehensive notice to employees and received their express consent.
- D. Consulted with the Information Security team to weigh security measures against possible server impacts.

Correct Answer: A

QUESTION 3

SCENARIO

Please use the following to answer the next question:

CreditPlaya, SA is an established Spanish online insurance company whose exclusive activity is providing health insurance for legal residents of Spain, regardless of their nationality.

CreditPlaya autonomously manages its own website, through which a potential customer, engaging in a free pre-contractual activity, enters his or her full name, e-mail address, tax identification number (to verify residence in Spain), age,

profession, and the full names of any other adult members of his or her family.

With this data, CreditPlaya immediately sends an email granting or denying eligibility for a health insurance policy. In the case of eligibility, the email also contains the eventual cost of the policy and two PDF documents – one with the contractual Terms and Conditions, and the other with the privacy notice as required by Article 13 of the GDPR. The CreditPlaya Information Tracking System (ITS) is very efficient, with a low rate of unpaid insurance policies. The ITS is automatically fed by the information provided by every applicant, whose data is then used to refine insurance policy rates.

To ensure their back-up procedures, in January 2021 CreditPlaya started sending weekly copies of the whole database with all the applicants' personal data to an independent company in Uruguay. The information was sent through state-of-the-art encrypting tools, but once in Uruguay was stored without any encryption method. In March 2022, the entire data base stored on the Uruguay's company servers was encrypted by malicious ransomware. There was no evidence that the data was accessed by unauthorized persons, much less altered or exfiltrated. Despite

the incident, CreditPlaya found that they could rely on the locally based Spanish back-up information and carry on its activity without interrupting its operations. The incident caused the termination of the professional relationship between the two companies.

If the data on the Uruguay company's servers had been encrypted, what kind of security measure would this be considered?

- A. A remediation security measure.
- B. A prevention security measure.
- C. A corrective security measure.
- D. A detection security measure.

Correct Answer: B

QUESTION 4

SCENARIO

Please use the following to answer the next question:

Jane starts her new role as a Data Protection Officer (DPO) at a Malta-based company that allows anyone to buy and sell cryptocurrencies via its online platform. The company stores and processes the personal data of its customers in a

dedicated data center located in Malta (EU).

People wishing to trade cryptocurrencies are required to open an online account on the platform. They then must successfully pass a Know Your Customer (KYC) due diligence procedure aimed at preventing money laundering and ensuring

compliance with applicable financial regulations.

The non-European customers are also required to waive all their GDPR rights by reading a disclaimer written in bold and ticking a checkbox on a separate page in order to get their account approved on the platform.

All customers must likewise accept the terms of service of the platform. The terms of service also include a privacy policy section, saying, among other things, that if a customer fails the KYC process, its KYC data will be automatically shared

with the national anti-money laundering agency.

The KYC procedure requires customers to answer many questions, including whether they have any criminal convictions, whether they use recreational drugs or have problems with alcohol, and whether they have a terminal illness. While

providing this data, customers see a conspicuous message saying that this data is meant only to prevent fraud and account takeover, and will be never shared with private third parties.

The company regularly conducts external security testing of its online systems by independent cybersecurity companies from the EU. At the final stage of testing, the company provides cybersecurity assessors with access to its central

database to review security permissions, roles and policies. Personal data in the database is encrypted; however, cybersecurity assessors usually have access to the decryption keys obtained while running initial security testing. The

assessors must strictly follow the guidelines imposed by the company during the entire testing and auditing process.

All customer data, including trading activities and all internal communications with technical support, are permanently stored in a secured AWS S3 Glacier cloud data storage, located in Ireland, for backup and compliance purposes. The data

is securely transferred to the cloud and then is properly encrypted while at rest by using AWS-native encryption mechanisms. These mechanisms give AWS the necessary technical means to encrypt and decrypt the data when such is

required by the company. There is no data processing agreement between AWS and the company.

Should Jane modify the required GDPR rights waiver for non-European residents?

A. Yes, the waiver must not apply to any residents of countries with an adequacy decision from the EC.



- B. Yes, this clause must be entirely removed as all customers, regardless of residence or nationality, shall enjoy the same individual rights granted under GDPR.
- C. No, the non-EU residents are not protected by GDPR unless they are physically located in the EU.
- D. No, but all non-EU residents must manually sign a separate waiver to ensure its lawfulness and enforceability under GDPR.

Correct Answer: B

QUESTION 5

SCENARIO Please use the following to answer the next question:

Gentle Hedgehog Inc. is a privately owned website design agency incorporated in Italy. The company has numerous remote workers in different EU countries. Recently, the management of Gentle Hedgehog noticed a decrease in productivity

of their sales team, especially among remote workers. As a result, the company plans to implement a robust but privacy-friendly remote surveillance system to prevent absenteeism, reward top performers, and ensure the best quality of

customer service when sales people are interacting with customers.

Gentle Hedgehog eventually hires Sauron Eye Inc., a Chinese vendor of employee surveillance software whose European headquarters is in Germany. Sauron Eye's software provides powerful remote-monitoring capabilities, including 24/7

access to computer cameras and microphones, screen captures, emails, website history, and keystrokes. Any device can be remotely monitored from a central server that is securely installed at Gentle Hedgehog headquarters. The

monitoring is invisible by default; however, a so-called Transparent Mode, which regularly and conspicuously notifies all users about the monitoring and its precise scope, also exists. Additionally, the monitored employees are required to use

a built-in verification technology involving facial recognition each time they log in.

All monitoring data, including the facial recognition data, is securely stored in Microsoft Azure cloud servers operated by Sauron Eye, which are physically located in France.

Under what condition could the surveillance system be used on the personal devices of employees?

- A. Only if the monitoring system is manufactured by a European vendor storing the monitoring data within the EU.
- B. Only if the employees give valid consent and the monitoring is narrowly limited to their professional tasks.
- C. Only if the cloud that stores the monitoring data is certified by the EDPB as GDPR compliant.
- D. Only if the employer offers an adequate compensation for using the employee's devices.

Correct Answer: B