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.geekcert.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

A German data subject was the victim of an embarrassing prank 20 years ago. A newspaper website published an article about the prank at the time, and the article is still available on the newspaper\\'s website. Unfortunately, the prank is the top search result when a user searches on the victim\\'s name. The data subject requests that SearchCo delist this result. SearchCo agrees, and instructs its technology team to avoid scanning or indexing the article. What else must SearchCo do?

A. Notify the newspaper that its article it is delisting the article.

B. Fully erase the URL to the content, as opposed to delist which is mainly based on data subject\\'s name.

C. Identify other controllers who are processing the same information and inform them of the delisting request.

D. Prevent the article from being listed in search results no matter what search terms are entered into the search engine.

Correct Answer: C

QUESTION 2

In the wake of the Schrems II ruling, which of the following actions has been recommended by the EDPB for companies transferring personal data to third countries?

A. Adopting a risk-based approach and implementing supplementary measures as needed.

B. Ensuring that all data transfers are encrypted with unbreakable encryption algorithms.

C. Obtaining explicit consent from each EU citizen for every individual data transfer.

D. Storing all personal data within the borders of the European Union.

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-ofthe-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.

The privacy notice provided by CreditPlaya contravenes Article 13 of the GDPR because?

A. The document is delivered after the personal data has been obtained.

B. The document is separated from the document listing Terms and Conditions.

C. The document is not written in the language of the average prospective customer.

D. The document fails to mention the applicable security measures for the processing.

Correct Answer: A

QUESTION 4

A news website based m (he United Slates reports primarily on North American events The website is accessible to any user regardless of location, as the website operator does not block connections from outside of the U.S. The website offers a pad subscription that requires the creation of a user account; this subscription can only be paid in U.S. dollars.

Which of the following explains why the website operator, who is the responsible for all processing related to account creation and subscriptions, is NOT required to comply with the GDPR?

A. Payments cannot be made in a European Union currency.

B. The controller does not have an establishment in the European Union.

C. The website is not available in several official languages of European Un on Member States

D. The website cannot block connections from outside the U.S. that use a Virtual Private Network (VPN) to simulate a US location.

Correct Answer: B

QUESTION 5

What is the most frequently used mechanism for legitimizing cross-border data transfer?

A. Standard Contractual Clauses.

B. Approved Code of Conduct.

C. Binding Corporate Rules.

D. Derogations.

Correct Answer: A

Reference: https://www.dataguidance.com/opinion/international-eu-us-cross-border-data-transfers