

# CIPP-E<sup>Q&As</sup>

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.certbus.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

### 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.

What is potentially wrong with the backup system operated in the AWS cloud?

A. The AWS servers are located in the EU but in a country different than the location of the corporate headquarters.

- B. It is unlawful to process any personal data in a cloud unless the cloud is certified as GDPR-compliant by a competent supervisory authority.
- C. The data storage period has to be revised, and a data processing agreement w\*h AWS must be signed
- D. AWS is a U S company, and no personal data of European residents may be transferred to it without explicit written consent from data subjects.

Correct Answer: C

---

### QUESTION 2

How is the GDPR's position on consent MOST likely to affect future app design and implementation?

- A. App developers will expand the amount of data necessary to collect for an app's functionality.
- B. Users will be given granular types of consent for particular types of processing.
- C. App developers' responsibilities as data controllers will increase.
- D. Users will see fewer advertisements when using apps.

Correct Answer: B

---

### QUESTION 3

According to the European Data Protection Board, controllers responding to a data subject access request can refuse to provide a copy of personal data under certain conditions. Which of the following is NOT one of these conditions?

- A. If the data subject access request was sent to an employee that is not involved in the processing of such requests.
- B. If there is such a large amount of data that the controller cannot identify the data subject of the request.
- C. If the controller is unable to use end-to-end encrypted emails for responding to such requests.
- D. If the personal data was processed in the past but is no longer at the controller's disposal at the time of the request.

Correct Answer: C

---

### QUESTION 4

Higher fines are assessed for GDPR violations due to which of the following?

- A. Failure to notify a supervisory authority and data subjects of a personal data breach
- B. Violations of a data controller's obligations to obtain a child's consent
- C. Failure to appoint a data protection officer.

D. Violations of a data subject's rights

Correct Answer: D

---

#### QUESTION 5

Under Article 30 of the GDPR, controllers are required to keep records of all of the following EXCEPT?

- A. Incidents of personal data breaches, whether disclosed or not.
- B. Data inventory or data mapping exercises that have been conducted.
- C. Categories of recipients to whom the personal data have been disclosed.
- D. Retention periods for erasure and deletion of categories of personal data.

Correct Answer: A

Reference: <https://medium.com/golden-data/what-records-must-controllers-and-processors-keep-to-comply-with-eu-data-protection-law-3e8bac177695>

---

#### QUESTION 6

If two controllers act as joint controllers pursuant to Article 26 of the GDPR, which of the following may NOT be validly determined by said controllers?

- A. The definition of a central contact point for data subjects.
- B. The rules regarding the exercising of data subjects' rights.
- C. The rules to provide information to data subjects in Articles 13 and 14.
- D. The non-disclosure of the essence of their arrangement to data subjects

Correct Answer: D

---

#### QUESTION 7

To which of the following parties does the territorial scope of the GDPR NOT apply?

- A. All member countries of the European Economic Area.
- B. All member countries party to the Treaty of Lisbon.
- C. All member countries party to the Paris Agreement.
- D. All member countries of the European Union.

Correct Answer: C

Reference: <https://www.complianceweek.com/understanding-the-territorial-scope-of-the-gdpr/24693.article>

---

### QUESTION 8

Article 58 of the GDPR describes the power of supervisory authorities. Which of the following is NOT among those granted?

- A. Legislative powers.
- B. Corrective powers.
- C. Investigatory powers.
- D. Authorization and advisory powers.

Correct Answer: A

Reference: <https://www.privacy-regulation.eu/en/article-58-powers-GDPR.htm>

---

### QUESTION 9

#### SCENARIO

Please use the following to answer the next question:

Javier is a member of the fitness club EVERFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Javier lives in Newry, Northern Ireland (part of the

U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Javier was photographed while working out at a branch of EVERFIT in Frankfurt, Germany. At the time, Javier gave his consent to

being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However,

the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Javier no longer feels comfortable with his photograph being publicly

associated with the fitness club.

After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Javier sends a letter to EVERFIT requesting that his image be removed from the website and all promotional materials.

Months pass and Javier, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact EVERFIT through alternate channels, he decides to take action against the company.

Javier contacts the U.K. Information Commissioner's Office (ICO, the U.K.'s supervisory authority) to lodge a complaint about this matter. The ICO, pursuant to Article 56 (3) of the GDPR, informs the CNIL (i.e. the supervisory authority of

EVERFIT's main establishment) about this matter. Despite the fact that EVERFIT has an establishment in the U.K., the CNIL decides to handle the case in accordance with Article 60 of the GDPR. The CNIL liaises with the ICO, as relevant

under the cooperation procedure. In light of issues amongst the supervisory authorities to reach a decision, the European Data Protection Board becomes involved and, pursuant to the consistency mechanism, issues a binding decision.

Additionally, Javier sues EVERFIT for the damages caused as a result of its failure to honor his request to have his photograph removed from the brochure and website.

Under the cooperation mechanism, what should the lead authority (the CNIL) do after it has formed its view on the matter?

- A. Submit a draft decision to other supervisory authorities for their opinion.
- B. Request that the other supervisory authorities provide the lead authority with a draft decision for its consideration.
- C. Submit a draft decision directly to the Commission to ensure the effectiveness of the consistency mechanism.
- D. Request that members of the seconding supervisory authority and the host supervisory authority co-draft a decision.

Correct Answer: A

---

#### QUESTION 10

An organisation receives a request multiple times from a data subject seeking to exercise his rights with respect to his own personal data. Under what condition can the organisation charge the data subject for processing the request?

- A. Only where the organisation can show that it is reasonable to do so because more than one request was made.
- B. Only to the extent this is allowed under the restrictions on data subjects' rights introduced under Art 23 of GDPR.
- C. Only where the administrative costs of taking the action requested exceeds a certain threshold.
- D. Only if the organisation can demonstrate that the request is clearly excessive or misguided.

Correct Answer: D

---

#### QUESTION 11

##### SCENARIO

Please use the following to answer the next question:

Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts. Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.

Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.

Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.

Why would the consent provided by Ms. Iman NOT be considered valid in regard to JaphSoft?

- A. She was not told which controller would be processing her personal data.
- B. She only viewed the visual representations of the privacy notice Liem provided.
- C. She did not read the privacy notice stating that her personal data would be shared.
- D. She has never made any purchases from JaphSoft and has no relationship with the company.

Correct Answer: C

---

## QUESTION 12

Which kind of privacy notice, originally advocated by the Article 29 Working Party, is commonly recommended for AI-based technologies because of the way it provides processing information at specific points of data collection?

- A. Privacy dashboard notice
- B. Visualization notice.
- C. Just-in-time notice.
- D. Layered notice.

Correct Answer: C

---

## QUESTION 13

### SCENARIO

Please use the following to answer the next question:

TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.

During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed Questionnaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories ?age, income, ethnicity ?that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the Questionnaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.

Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.

If TripBliss Inc. decides not to report the incident to the supervisory authority, what would be their BEST defense?

- A. The resulting obligation to notify data subjects would involve disproportionate effort.
- B. The incident resulted from the actions of a third-party that were beyond their control.
- C. The destruction of the stolen data makes any risk to the affected data subjects unlikely.
- D. The sensitivity of the categories of data involved in the incident was not substantial enough.

Correct Answer: C

---

#### QUESTION 14

Which of the following is NOT recognized as being a common characteristic of cloud-computing services?

- A. The service's infrastructure is shared among the supplier's customers and can be located in a number of countries.
- B. The supplier determines the location, security measures, and service standards applicable to the processing.
- C. The supplier allows customer data to be transferred around the infrastructure according to capacity.
- D. The supplier assumes the vendor's business risk associated with data processed by the supplier.



Correct Answer: D

Reference: <https://www.softwaremajor.com/news-articles/64-gdpr-how-does-it-apply-to-the-cloud>

## QUESTION 15

### SCENARIO

Please use the following to answer the next question:

WonderkKids provides an online booking service for childcare. Wonderkids is based in France, but hosts its website through a company in Switzerland. As part of their service, WonderKids will pass all personal data provided to them to the childcare provider booked through their system. The type of personal data collected on the website includes the name of the person booking the childcare, address and contact details, as well as information about the children to be cared for including name, age, gender and health information. The privacy statement on Wonderkids\ website states the following:

"WonderkKids provides the information you disclose to us through this website to your childcare provider for scheduling and health and safety reasons. We may also use your and your child's personal information for our own legitimate business purposes and we employ a third-party website hosting company located in Switzerland to store the data. Any data stored on equipment located in Switzerland meets the European Commission provisions for guaranteeing adequate safeguards for you and your child's personal information. We will only share you and your child's personal information with businesses that we see as adding real value to you. By providing us with any personal data, you consent to its transfer to affiliated businesses and to send you promotional offers."

"We may retain you and your child's personal information for no more than 28 days, at which point the data will be depersonalized, unless your personal information is being used for a legitimate business purpose beyond 28 days where it may be retained for up to 2 years."

"We are processing you and your child's personal information with your consent. If you choose not to provide certain information to us, you may not be able to use our services. You have the right to: request access to you and your child's personal information; rectify or erase you or your child's personal information; the right to correction or erasure of you and/or your child's personal information; object to any processing of you and your child's personal information. You also have the right to complain to the supervisory authority about our data processing activities."

What must the contract between WonderKids and the hosting service provider contain?

- A. The requirement to implement technical and organizational measures to protect the data.
- B. Controller-to-controller model contract clauses.
- C. Audit rights for the data subjects.
- D. A non-disclosure agreement.

Correct Answer: B