

# New CIPP-E Braindumps Questions, CIPP-E Downloadable PDF

## CIPP/E Questions and Answers

### 1. Universal Declaration of Human Rights - Passage

ANS 1948

### 2. Universal Declaration of Human Rights - Article 12

ANS The right to a private life and associated freedoms.

### 3. Universal Declaration of Human Rights - Article 19

ANS Freedom of expression.

### 4. Universal Declaration of Human Rights - Article 29(2)

ANS Rights are not absolute and there are instances where a balance must be struck.

### 5. European Convention on Human Rights

ANS Treaty drawn up by the Council of Europe that protects fundamental rights. Adopted in 1953 and based on the Universal Declaration of Human Rights.

### 6. European Convention on Human Rights - Enforcement

ANS Enforced by the European Court of Human Rights

### 7. European Convention on Human Rights - Article 8

ANS Protects rights of individuals

1 / 10

BTW, DOWNLOAD part of TrainingDump CIPP-E dumps from Cloud Storage: <https://drive.google.com/open?id=1sJdkWp59IVZpE9znbrqwsOMnJYl2VbeK>

As we all know, the CIPP-E certificate has a very high reputation in the global market and has a great influence. But how to get the certificate has become a headache for many people. Our CIPP-E learning materials provide you with an opportunity. Once you choose our CIPP-E Exam Practice, we will do our best to provide you with a full range of thoughtful services. Whenever you have questions about our CIPP-E study guide, our service will give you the most professional advice.

## IAPP CIPP-E Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>Information Systems Auditing Process: This section of the exam measures skills of an IT Auditor and covers how to plan, conduct, and report on audits of information systems. It tests ability to use audit standards, gather evidence, do sampling, manage audit engagements, and ensure audit quality.</li></ul>

Topic 2	<ul style="list-style-type: none"> <li>• Information Systems Operations &amp; Business Resilience: This domain focuses on an IT Manager's responsibilities in operations: maintaining systems, managing assets, ensuring availability and capacity, handling incidents and changes, performing business continuity planning, disaster recovery, and ensuring resilience of IT services</li> </ul>
Topic 3	<ul style="list-style-type: none"> <li>• Information Systems Acquisition, Development &amp; Implementation: Here, the exam assesses an IT Auditor's knowledge about acquiring or building new systems, understanding project governance, evaluating development methodologies, ensuring systems are properly tested and implemented, and verifying that changes meet requirements.</li> </ul>
Topic 4	<ul style="list-style-type: none"> <li>• Protection of Information Assets: This part measures an IT Auditor's expertise in protecting data and systems. It includes understanding of identity and access management, data encryption, endpoint and network security, physical</li> <li>• environmental controls, threat detection and incident response, and ensuring compliance with security frameworks.</li> </ul>
Topic 5	<ul style="list-style-type: none"> <li>• Governance &amp; Management of IT: This section evaluates the capabilities of an IT Manager in overseeing IT governance, defining policies and procedures, aligning IT strategy with business objectives, handling enterprise risk management, and managing IT resources and vendor relationships.</li> </ul>

>> New CIPP-E Braindumps Questions <<

## CIPP-E Downloadable PDF & Test CIPP-E Objectives Pdf

When new changes or knowledge are updated, our experts add additive content into our CIPP-E latest material. They have always been in a trend of advancement. Admittedly, our CIPP-E real questions are your best choice. We also estimate the following trend of exam questions may appear in the next exam according to syllabus. So they are the newest and also the most trustworthy CIPP-E Exam Prep to obtain.

IAPP CIPP-E (Certified Information Privacy Professional/Europe) exam is a certification program that aims to provide individuals with a comprehensive understanding of data protection laws and regulations in Europe. Certified Information Privacy Professional/Europe (CIPP/E) certification program is designed for privacy professionals who are responsible for managing and implementing data protection policies within their organizations. CIPP-E Exam covers a wide range of topics, including the EU General Data Protection Regulation (GDPR), the role of data protection officers, cross-border data transfers, and data subject rights.

### IAPP Certified Information Privacy Professional/Europe (CIPP/E) Sample Questions (Q191-Q196):

#### NEW QUESTION # 191

A private company has establishments in France, Poland, the United Kingdom and, most prominently, Germany, where its headquarters is established. The company offers its services worldwide. Most of the services are designed in Germany and supported in the other establishments. However, one of the services, a Software as a Service (SaaS) application, was defined and implemented by the Polish establishment. It is also supported by the other establishments.

What is the lead supervisory authority for the SaaS service?

- A. The supervisory authority of Germany at regional level.
- B. The supervisory authority of Germany at federal level.
- **C. The supervisory authority of the Republic of Poland.**
- D. The supervisory authority of the European Union.

**Answer: C**

Explanation:

According to the GDPR, the lead supervisory authority (LSA) is the one located in the EU member state where the controller or processor has its main establishment or single establishment. The main establishment is the place where the decisions on the purposes and means of the processing of personal data are taken. In this case, the SaaS service was defined and implemented by the Polish

establishment, so the decisions on the processing of personal data for this service are taken in Poland. Therefore, the LSA for the SaaS service is the supervisory authority of the Republic of Poland.

Reference:

GDPR Article 4(16): Definition of main establishment

GDPR Article 56: Competence of the lead supervisory authority

GDPR Recital 36: Determination of the main establishment

IAPP CIPP/E Study Guide, Chapter 5, Section 5.1: Lead Supervisory Authority

### NEW QUESTION # 192

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. Notify law enforcement and consult with legal counsel to understand the implications of the breach and the notification requirements.
- D. Wait for law enforcement to provide guidance on notification procedures before taking any further action.

**Answer: A**

Explanation:

After determining the scope of a ransomware attack, the organization should assess the risks associated with the breach. This risk assessment will help determine whether notification of affected individuals and regulatory bodies is required. If notification is required, it should be done within the relevant timeframes.

Reference:

IAPP CIPP/E textbook, Chapter 5: Data Breach Notification

IAPP CIPP/E Study Guide, Domain 3: Incident Response

### NEW QUESTION # 193

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

**Answer: C**

### NEW QUESTION # 194

Pursuant to Article 17 and EDPB Guidelines S'2019 on RTBF criteria in search engines cases, all of the following would be valid grounds for data subject delisting requests EXCEPT?

- A. The data subject withdraws consent and there is no other legal basis for the processing.
- B. The personal data is no longer necessary in relation to the search engine provider's processing
- C. The personal data has been collected in relation to the offer of information society services (ISS) to a child.
- **D. The processing is necessary for exercising the right of freedom of expression and information**

**Answer: D**

Explanation:

According to Article 17 of the GDPR, the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller has the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing; the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). However, Article 17(3) provides that the right to erasure does not apply to the extent that processing is necessary for exercising the right of freedom of expression and information. Therefore, this would not be a valid ground for data subject delisting requests. Reference:

Article 17 of the GDPR

EDPB Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)

### NEW QUESTION # 195

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.

Assuming that multiple EVERFIT branches across several EU countries are acting as separate data controllers, and that each of those branches were responsible for mishandling Javier's request, how may Javier proceed in order to seek compensation?

- A. He will be able to apply to the European Data Protection Board in order to determine which particular EVERFIT branch is liable for damages, based on the decision that was made by the board.
- **B. He will be able to sue any one of the relevant EVERFIT branches, as each one may be held liable for the entire damage.**

