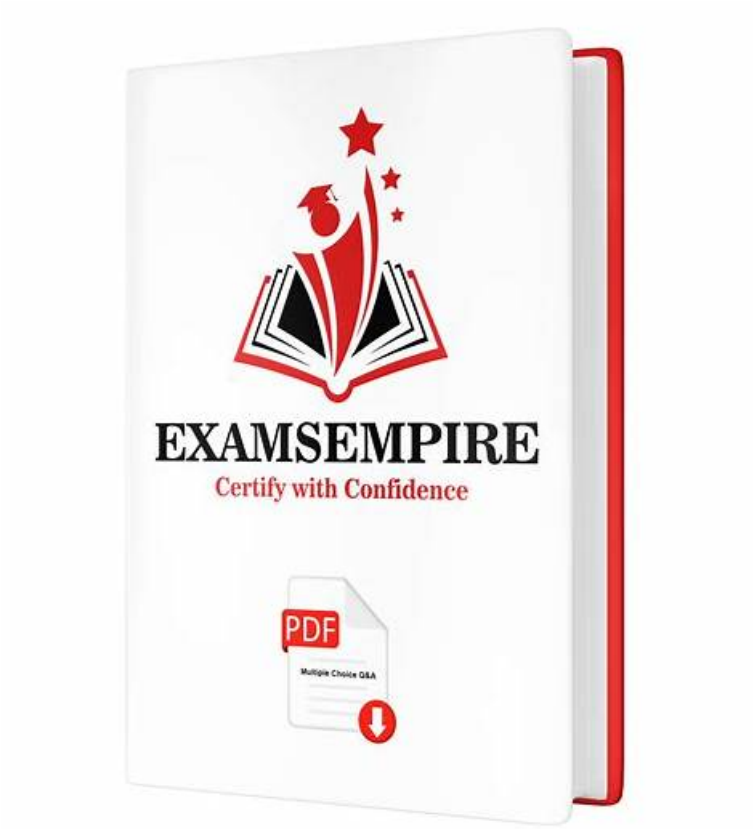
CIPP-E Real Dump | CIPP-E Exam Quiz



DOWNLOAD the newest Real4dumps CIPP-E PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1JXWMJSMI0OCMszZTn3wEb9bMYnULnhLp

To assist applicants preparing for the Certified Information Privacy Professional/Europe (CIPP/E) (CIPP-E) real certification exam effectively, Real4dumps offers IAPP CIPP-E desktop practice test software and a web-based practice exam besides actual PDF CIPP-E exam questions. These CIPP-E Practice Exams replicate the IAPP CIPP-E real exam scenario and offer a trusted evaluation of your preparation. No internet connection is necessary to use the CIPP-E Windows-based practice test software.

IAPP CIPP-E (Certified Information Privacy Professional/Europe) Certification Exam is a globally recognized certification for professionals who are involved in managing and protecting personal data in Europe. Certified Information Privacy Professional/Europe (CIPP/E) certification is designed to equip professionals with the knowledge and skills to navigate the complex legal and regulatory landscape of data privacy in Europe. It covers a range of topics such as GDPR (General Data Protection Regulation), data protection laws and regulations, data breaches, privacy by design, and more.

>> CIPP-E Real Dump <<

CIPP-E Exam Dumps & CIPP-E Dumps Guide & CIPP-E Best Questions

In order to help you control the CIPP-E examination time, we have considerately designed a special timer to help your adjust the pace of answering the questions of the CIPP-E study materials. Many people always are stopped by the difficult questions. Then they will fall into thoughts to try their best to answer the questions of the CIPP-E Real Exam. But they forgot to answer the other questions, our CIPP-E training guide can help you solve this problem and get used to the pace.

The CIPP-E Certification Exam is ideal for professionals who work with personal data in Europe or who have responsibilities for data protection compliance. CIPP-E exam covers a wide range of topics, including the legal and regulatory framework for data protection in Europe, data protection principles and practices, privacy program management, and data breach management. Certified Information Privacy Professional/Europe (CIPP/E) certification is intended to equip professionals with the knowledge and skills necessary to develop and implement effective data protection strategies in their organizations.

IAPP Certified Information Privacy Professional/Europe (CIPP/E) Sample Questions (Q208-Q213):

NEW QUESTION # 208
When is data sharing agreement MOST likely to be needed?

- A. When personal data is being shared with a public authority with powers to require the personal data to be disclosed.
- B. When personal data is being proactively shared by a controller to support a police investigation.
- C. When personal data is being shared between commercial organizations acting as joint data controllers.
- D. When anonymized data is being shared.

Answer: C

NEW QUESTION # 209
Which of the following countries will continue to enjoy adequacy status under the GDPR, pending any future European Commission decision to the contrary?

- A. Switzerland
- B. Norway
- C. Australia
- D. Greece

Answer: A

Explanation:
Adequacy is a term that the EU uses to describe other countries, territories, sectors or international organisations that it deems to provide an 'essentially equivalent' level of data protection to that which exists within the EU. An adequacy decision is a formal decision made by the EU which recognises that another country, territory, sector or international organisation provides an equivalent level of protection for personal data as the EU does. The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary12.
The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay as providing adequate protection13. On 28 June 2021, the EU Commission published two adequacy decisions in respect of the UK: one for transfers under the EU GDPR; and the other for transfers under the Law Enforcement Directive (LED)2. These decisions contain the European Commission's detailed assessment of the UK's laws and systems for protecting personal data, as well as the legislation designating the UK as adequate. Both adequacy decisions are expected to last until 27 June 20252.
Among the four options given, only Switzerland has been granted an adequacy decision by the EU, which means that it will continue to enjoy adequacy status under the GDPR, pending any future European Commission decision to the contrary. Greece is a member state of the EU, so it does not need an adequacy decision to receive personal data from the EU. Norway is a member of the European Economic Area (EEA), which also includes Iceland and Liechtenstein, and has incorporated the GDPR into its national law, so it also does not need an adequacy decision. Australia has not been recognised as adequate by the EU, so transfers of personal data from the EU to Australia require appropriate safeguards or derogations13. Therefore, the correct answer is D. Switzerland. References:
https://pages.iapp.org/Free-Study-Guides_CIPPE-PPC-EU.htmlhttps://data-privacy-office.eu/courses/cipp-e- official-training-course/ Reference: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/ adequacy-decisions_en

NEW QUESTION # 210
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 federal level.
- B. The supervisory authority of Germany at regional 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.
References:
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 # 211
What is true of both the General Data Protection Regulation (GDPR) and the Council of Europe Convention 108?

- A. Both require notification of processing activities to a supervisory authority
- B. Both govern international transfers of personal data
- C. Both govern the manual processing of personal data
- D. Both only apply to European Union countries

Answer: A

Explanation:
The GDPR and the Convention 108 are two important data protection instruments that aim to protect the rights and freedoms of individuals with regard to their personal data. They both have some similarities and some differences, but one common feature is that they both require notification of processing activities to a supervisory authority.
A supervisory authority is an independent public body that monitors and enforces compliance with data protection laws. In the EU, there are 47 national data protection authorities (DPAs) that have the power to impose administrative fines, issue guidelines, conduct investigations, and cooperate with other authorities1. In the Council of Europe, there are 54 parties to the Convention 108 that have established their own supervisory authorities or have agreed to be supervised by an external authority2.
Notification of processing activities is a requirement for any controller or processor of personal data that falls under the scope of the GDPR or the Convention 108. A controller is a natural or legal person who determines the purposes and means of the processing of personal data3. A processor is a natural or legal person who processes personal data on behalf of a controller3. Notification means informing the supervisory authority about certain aspects of the processing, such as:
* The identity and contact details of the controller and processor
* The categories and sources of personal data
* The purposes and legal basis for processing
* The recipients or categories of recipients of personal data
* The retention period or criteria for determining it
* The existence of any automated decision-making or profiling
* The rights of data subjects and how they can exercise them
Notification can be done in various ways, such as:
* Submitting a written notification form
* Publishing a notice on a website or other platform
* Sending an email or other electronic message
* Using an online system or portal
Notification should be done as soon as possible after becoming aware of any relevant information about the processing. It should also be updated whenever there are significant changes in relation to the processing4.
Therefore, both the GDPR and the Convention 108 require notification of processing activities to a supervisory authority. This is one way to ensure transparency, accountability, and compliance with data protection laws.

NEW QUESTION # 212
Which of the following is NOT exempt from the material scope of the GDPR. insofar as the processing of personal data is concerned?

- A. A natural person in the course of activity conducted purely tor a personally-owned sole proprietorship.
- B. A natural person in the course of a large-scale but purely personal or household activity.
- C. A natural person processing data foe a small-scale, purely personal or household activity.
- D. A natural person in the course of processing purely personal or household data on behalf of a spouse who is beyond the age of majority.

Answer: B

Explanation:
The material scope of the GDPR is outlined in Article 21. The Regulation applies to 'processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.'1 However, the Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity1. This exemption is meant to protect the privacy of individuals in their private sphere and to exclude activities that have no connection with a professional or commercial activity2. The exemption covers activities such as correspondence, social networking, online publication of photos or videos, and the use of online services for personal purposes2. However, the exemption does not apply if the processing of personal data affects the rights and freedoms of others, such as when the data is made accessible to an indefinite number of people3. Therefore, the processing of personal data by a natural person in the course of a large-scale but purely personal or household activity is not exempt from the material scope of the GDPR, as it may have an impact on the privacy of other individuals. The other options are exempt from the material scope of the GDPR, as they involve small-scale, purely personal or household activities that do not affect the rights and freedoms of others.
References: 1: Article 2 of the GDPR2: Recital 18 of the GDPR3:
CJEU, Case C-101/01, Lindqvist, 2003.

NEW QUESTION # 213
......

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, Disposable vapes

BTW, DOWNLOAD part of Real4dumps CIPP-E dumps from Cloud Storage: https://drive.google.com/open?id=1JXWMJSMI0OCMszZTn3wEb9bMYnULnhLp