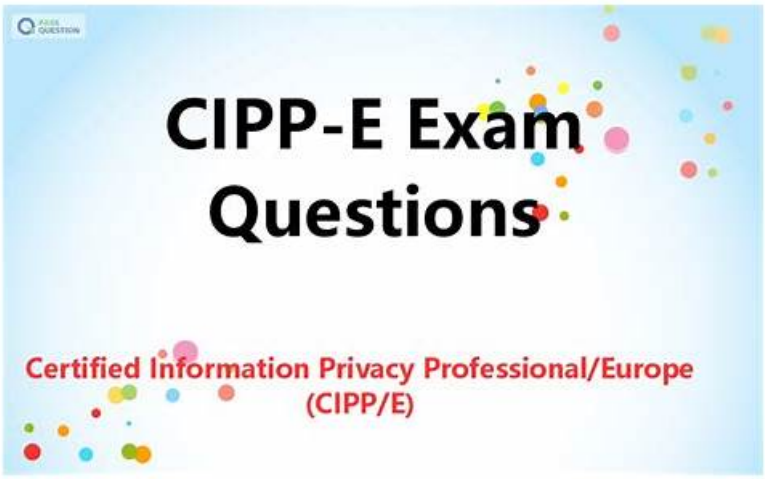
100% Pass Latest CIPP-E - New Certified Information Privacy Professional/Europe (CIPP/E) Braindumps Questions



What's more, part of that DumpsTests CIPP-E dumps now are free: https://drive.google.com/open?id=1ZULPEaL_wksjEnyB-vzQh379Di_WFDfN

The IAPP CIPP-E exam questions are being offered in three different formats. These formats are Certified Information Privacy Professional/Europe (CIPP/E) (CIPP-E) PDF dumps files, desktop practice test software, and web-based practice test software. All these three Certified Information Privacy Professional/Europe (CIPP/E) (CIPP-E) exam dumps formats contain the real Certified Information Privacy Professional/Europe (CIPP/E) (CIPP-E) exam questions that assist you in your Certified Information Privacy Professional/Europe (CIPP/E) (CIPP-E) practice exam preparation and finally, you will be confident to pass the final CIPP-E exam easily.

IAPP CIPP-E Exam is an important certification for professionals who work in data privacy in Europe. It tests a candidate's knowledge and understanding of the GDPR and other data protection laws, privacy principles, and data breaches. With the right preparation, candidates can successfully pass the exam and earn a highly-regarded certification that demonstrates their expertise in the field of data privacy.

>> New CIPP-E Braindumps Questions <<

HotNew CIPP-E Braindumps Questions & Leader in Qualification Exams & Updated IAPP Certified Information Privacy Professional/Europe (CIPP/E)

During nearly ten years, our CIPP-E exam questions have met with warm reception and quick sale in the international market. Our CIPP-E study materials are not only as reasonable priced as other makers, but also they are distinctly superior in the many respects. With tens of thousands of our loyal customers supporting us all the way, we believe we will do a better job in this career. More and more candidates will be benefited from our excellent CIPP-E training guide!

One of the key benefits of obtaining a CIPP-E Certification is that it demonstrates to employers and clients that an individual has a deep understanding of privacy and data protection laws and regulations. This can be particularly valuable given the increasing importance of privacy and data protection in today's digital world, where data breaches and privacy violations are becoming more common.

IAPP Certified Information Privacy Professional/Europe (CIPP/E) Sample Questions (Q69-Q74):

NEW QUESTION # 69
What is one major goal that the OECD Guidelines, Convention 108 and the Data Protection Directive (Directive 95/46/EC) all had in common but largely failed to achieve in Europe?

- A. The restriction of cross-border data flow
- B. The synchronization of approaches to data protection
- C. The establishment of a list of legitimate data processing criteria
- D. The creation of legally binding data protection principles

Answer: A

Explanation:
Explanation/Reference: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf (99)

NEW QUESTION # 70
The origin of privacy as a fundamental human right can be found in which document?

- A. Charier of Fundamental Rights of the European Union 2000.
- B. Universal Declaration of Human Rights 1948.
- C. European Convention of Human Rights 1953.
- D. OECD Guidelines on the Protection of Privacy 1980.

Answer: B

Explanation:
The Universal Declaration of Human Rights (UDHR) was adopted by the United Nations General Assembly in 1948 as a response to the atrocities of World War II. It is considered the first global expression of human rights and fundamental freedoms. Article 12 of the UDHR states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." This article is the origin of privacy as a fundamental human right that has influenced many subsequent international and regional instruments, such as the European Convention of Human Rights (ECHR), the OECD Guidelines on the Protection of Privacy, and the Charter of Fundamental Rights of the European Union (CFREU). Reference:
IAPP CIPP/E Study Guide, page 7
[Universal Declaration of Human Rights]
[Article 12 of the UDHR]

NEW QUESTION # 71
The GDPR's list of processor obligations regarding cloud computing includes all of the following EXCEPT?

- A. Individuals authorized to process the personal data are subject to an obligation of confidentiality.
- B. Controllers must be given notice of any subprocessors and have a right of objection.
- C. Processors must implement technical and organizational measures to ensure a level of security appropriate to the risk.
- D. Any personal data related to data subjects must be securely maintained for a maximum of ten years.

Answer: D

Explanation:
The General Data Protection Regulation (GDPR) introduces several obligations for processors who process personal data on behalf of controllers. These obligations apply to any processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services to data subjects in the EU or the monitoring of their behaviour as far as their behaviour takes place within the EU.
The GDPR's list of processor obligations regarding cloud computing includes all of the following:
Controllers must be given notice of any subprocessors and have a right of objection. According to Article 28 of the GDPR, a processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
Individuals authorized to process the personal data are subject to an obligation of confidentiality. According to Article 28 of the GDPR, the processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
Processors must implement technical and organizational measures to ensure a level of security appropriate to the risk. According to Article 32 of the GDPR, the processor shall implement appropriate technical and organisational measures to ensure a level of

security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.
The GDPR's list of processor obligations regarding cloud computing does not include the following:
Any personal data related to data subjects must be securely maintained for a maximum of ten years. The GDPR does not specify a precise time limit for the storage of personal data, but leaves it to the controller to determine the appropriate retention period, taking into account the nature, scope, context and purposes of the processing, as well as the risks for the rights and freedoms of data subjects. The GDPR also allows for the further storage of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to appropriate safeguards. Therefore, the processor must follow the instructions of the controller regarding the storage duration of the personal data, and delete or return the personal data to the controller after the end of the provision of services relating to the processing, unless required to store the personal data by Union or Member State law.
References:
GDPR, Articles 3, 4, 28, 29, 32, 51, 55, 56, 57, 58, 60, 61, 62, 63, 64, 65, 66, 67, and 68.
EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, pages 19, 20, 21, 22, 23, 24, 25, 26, 27, and 28.
Cloud Computing and GDPR: what you need to know | Combell, paragraphs 1, 2, 3, 4, 5, 6, 7, and 8.
GDPR Processor Obligations - Taylor Wessing, paragraphs 1, 2, 3, 4, 5, 6, 7, and 8.

NEW QUESTION # 72
Which of the following is NOT an explicit right granted to data subjects under the GDPR?

- A. The right to opt-out of the sale of their personal data to third parties.
- B. The right to request restriction of processing of personal data, under certain scenarios.
- C. The right to request the deletion of data a controller holds about them.
- D. The right to request access to the personal data a controller holds about them.

Answer: D

Explanation:
Reference https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/

NEW QUESTION # 73
Which of the following elements does NOT need to be presented to a data subject in order to collect valid consent for the use of cookies?

- A. A list of cookies that may be placed.
- B. Information on the purpose of the cookies.
- C. A "Cookies Settings" button.
- D. A "Reject All" cookies button.

Answer: C

Explanation:
According to the EDPB Guidelines 05/2020 on consent under Regulation 2016/6791, valid consent for the use of cookies must meet the following conditions:
*It must be freely given, which means that the data subject must have a genuine choice and the ability to refuse or withdraw consent without detriment.
*It must be specific, which means that the data subject must give consent for each distinct purpose of the processing and for each type of cookie.
*It must be informed, which means that the data subject must receive clear and comprehensive information about the identity of the controller, the purposes of the processing, the types of cookies used, the duration of the cookies, and the possibility of withdrawing consent.
*It must be unambiguous, which means that the data subject must express their consent by a clear affirmative action, such as clicking on an "I agree" button or selecting specific settings in a cookie banner.
*It must be granular, which means that the data subject must be able to consent to different types of cookies separately, such as essential, functional, performance, or marketing cookies.
Therefore, a "Cookies Settings" button is not a necessary element to collect valid consent for the use of cookies, as long as the data subject can exercise their choice and preference through other means, such as a cookie banner with different options. However, a "Cookies Settings" button may be a good practice to enhance transparency and user control, as it allows the data subject to access

and modify their consent settings at any time.
On the other hand, a "Reject All" cookies button is a necessary element to collect valid consent for the use of cookies, as it ensures that the data subject can freely refuse consent without detriment. A list of cookies that may be placed and information on the purpose of the cookies are also necessary elements to collect valid consent for the use of cookies, as they ensure that the data subject is informed and can give specific consent for each type of cookie.
References: EDPB Guidelines 05/2020 on consent under Regulation 2016/6791, pages 17-23.

NEW QUESTION # 74
.....