Free Questions for CIPP-E by dumpshq

Shared by Arnold on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SCENARIO

Please use the following to answer the next question:

Jane Stan's 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 m Malta |EU).

People wishing to trade cryptocurrencies are required to open an online account on the platform. They then must successfully pass a 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 belong a checkbox on a separate page in order to get their account approved on the platform.

The 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

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

Options:

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 GOPR-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.

Answer:

C

Explanation:

According to the GDPR, personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed1. Therefore, the data storage period of the backup system must be aligned with this principle and reviewed regularly.Moreover, the GDPR requires that when a controller (the company) uses a processor (AWS) to process personal data on its behalf, it must ensure that the processor provides sufficient guarantees to implement appropriate technical and organizational measures to meet the requirements of the GDPR and ensure the protection of the rights of the data subjects2.This is usually done by signing a data processing agreement that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller3.AWS offers a GDPR-compliant Data Processing Addendum (DPA) that is incorporated into the AWS Service Terms and applies automatically to all customers who require it to comply with the GDPR4.Reference:

Free CIPP/E Study Guide, page 24, section 4.2.1

Free CIPP/E Study Guide, page 25, section 4.3

GDPR, Article 28

GDPR - Amazon Web Services (AWS), section "GDPR resources"

Question 2

Question Type: **MultipleChoice**

SCENARIO

Please use the following to answer the next question:

Jane Stan's 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 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 belong a checkbox on a separate page in order to get their account approved on the platform.

The 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

Which of the following must be a component of the anti-money-laundering data-sharing practice of the platform?

Options:

A- The terms of service shall also enumerate all applicable anti-money laundering few.

B- Customers shall have an opt-out feature to restrict data sharing with law enforcement agencies after the registration.

C- The terms of service shall include the address of the anti-money laundering agency and contacts of the investigators who may access me data.

D- Customers snail receive a clear and conspicuous notice about such data sharing before submitting their data during the registration process.

Answer:

D

Explanation:

According to Article 13 of the GDPR, when personal data are collected from the data subject, the controller shall provide the data subject with certain information, such as the purposes and legal basis of the processing, the recipients or categories of recipients of the personal data, and the existence of the data subject's rights. This information shall be provided at the time when personal data are obtained. The

purpose of this requirement is to ensure that the data subject is informed and aware of how their personal data will be used and shared, and to enable them to exercise their rights accordingly. Therefore, customers shall receive a clear and conspicuous notice about such data sharing before submitting their data during the registration process.Reference:

Article 13 of the GDPR

IAPP CIPP/E Study Guide, page 32

Question 3

Question Type: **MultipleChoice**

SCENARIO

Please use the following to answer the next question:

Jane Stan's 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 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 belong a checkbox on a separate page in order to get their account approved on the platform.

The 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

Are the cybersecurity assessors required to sign a data processing agreement with the company in order to comply with the GDPR"

Options:

A- No, the assessors do not quality as data processors as they only have access to encrypted data.

B- No. the assessors do not quality as data processors as they do not copy the data to their facilities.

C- Yes. the assessors a-e considered to be joint data controllers and must sign a mutual data processing agreement.

D- Yes, the assessors are data processors and their processing of personal data must be governed by a separate contract or other legal act.

Answer:

D

Explanation:

According to the GDPR, a data processor is any person or entity that processes personal data on behalf of a data controller1.A data controller is the one who determines the purposes and means of the processing of personal data1.A data processing agreement (DPA) is a contractual document that sets out the rights and obligations of both parties regarding data protection2.The GDPR requires that a data controller who engages a data processor must enter into a written contract or legal act along the lines set out in Article 28.3 of the GDPR3.The DPA must specify, among other things, the subject matter, duration, nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller3.

In this scenario, the company is the data controller, as it determines the purposes and means of processing the personal data of its customers. The cybersecurity assessors are data processors, as they process the personal data of the customers on behalf of the company. The assessors have access to the personal data, even if it is encrypted, and they perform a specific technical service for the company. Therefore, the assessors are required to sign a DPA with the company in order to comply with the GDPR.The DPA will define the scope, nature and purpose of the processing, the security measures to be implemented, the notification procedures in case of a data breach, and the rights and obligations of both parties.Reference:1: Article 4 of the GDPR2: Data Processing Agreement (Template) - GDPR.eu3: Article 28 of the GDPR.

Question 4

Question Type: MultipleChoice

What was the main failing of Convention 108 that led to the creation of the Data Protection Directive (Directive 95/46/EC)?

Options:

A- IT did not account for the rapid growth of the Internet

B- It did not include protections for sensitive personal data

C- It was implemented in a fragmented manner by a small number of states.

D- Its penalties for violations of data protection rights were widely viewed as r sufficient.

Answer:

C

Explanation:

Convention 108 was the first legally binding international instrument in the data protection field, adopted by the Council of Europe in 19811.However, it had some limitations that led to the creation of the Data Protection Directive (Directive 95/46/EC) by the European Union in 19952.One of the main failings of Convention 108 was that it was implemented in a fragmented manner by a small number of states, resulting in divergent and inconsistent national laws and practices3.The Data Protection Directive aimed to harmonize the data protection rules within the EU and to ensure a high level of protection for individuals' rights and freedoms2. Therefore, option C is the correct answer.Option A is incorrect because Convention 108 did account for the rapid growth of the Internet by allowing for amendments and protocols to adapt to technological developments1.Option B is incorrect because Convention 108 did include protections for sensitive personal data, such as those revealing racial origin, political opinions, religious beliefs, health, or sexual life1.Option D is incorrect because Convention 108 did not prescribe specific penalties for violations of data protection rights, but left it to the Parties to adopt appropriate sanctions and remedies1.Reference:

Convention 108 and Protocols

CIPP/E Certification

Convention 108+ and the Data Protection Framework of the EU

Question 5

Question Type: MultipleChoice

Which of the following regulates the use of electronic communications services within the European Union?

Options:

A- Regulator (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015.

B- Regulation (EU) 2017/1953 of the European Parliament and of the Council of 25 October 2017.

C- Directive 2002/58'EC of the European Parliament and of the Council of 12 July 2002.

D- Directive (EU) 2019.789 of the European Parliament and of the Council of 17 April 2019.

Answer:

C

Explanation:

Directive 2002/58/EC, also known as the ePrivacy Directive, regulates the use of electronic communications services within the European Union. It covers issues such as confidentiality of communications, processing of traffic and location data, spam, cookies, and security breaches. It complements and particularises Directive 95/46/EC, also known as the Data Protection Directive, which sets out the general principles for the protection of personal data in the EU. The ePrivacy Directive was amended by Directive 2009/136/EC, which introduced new provisions on consent, cookies, and breach notification. The ePrivacy Directive is currently under review and will be replaced by a new Regulation on Privacy and Electronic Communications (ePrivacy Regulation), which is still being negotiated by the EU institutions.Reference:Directive 2002/58/EC,Directive 2009/136/EC, [ePrivacy Regulation]

Question 6

Question Type: MultipleChoice

Which statement provides an accurate description of a directive?

Options:

A- A directive speo5es certain results that must be achieved, but each member state is free to decide how to turn it into a national law

B- A directive has binding legal force throughout every member state and enters into force on a set date in all the member states.

C- A directive is a legal act relating to specific cases and directed towards member states, companies 0' private individuals.

D- A directive is a legal act that applies automatically and uniformly to all EU countries as soon as it enters into force.

Answer:

A

Explanation:

According to the EU glossary1, a directive is a legal act that sets out a goal that EU countries must achieve, but leaves them the choice of form and methods to reach it. A directive is binding on the EU countries to which it is addressed, but it does not apply directly at the national level. Instead, it has to be transposed into national law by the national authorities, usually within a specified time limit. This allows for some flexibility and adaptation to the specific circumstances of each country. A directive is different from a regulation, which is a legal act that applies automatically and uniformly to all EU countries as soon as it enters into force, without needing to be transposed into national law.Reference:

Free CIPP/E Study Guide, page 14, section 2.3

Types of legislation, section 2

What are EU directives?

Question 7

Question Type: MultipleChoice

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

Options:

A- Universal Declaration of Human Rights 1948.

B- European Convention of Human Rights 1953.

C- OECD Guidelines on the Protection of Privacy 1980.

D- Charier of Fundamental Rights of the European Union 2000.

Answer:

A

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]

Question 8

Question Type: MultipleChoice

According to the GDPR, when should the processing of photographs be considered processing of special categories of personal data?

Options:

A- When processed with the intent to publish information regarding a natural person on publicly accessible media.

B- When processed with the intent to proceed to scientific or historical research projects.

C- When processed with the intent to uniquely identify or authenticate a natural person.

D- When processed with the intent to comply with a law.

Answer:

C

Explanation:

:According to the GDPR, the processing of photographs should not systematically be considered as processing of special categories of personal data, unless they are covered by the definition of biometric data1.Biometric data is defined as personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification or authentication of that natural person, such as facial images or dactyloscopic data2.Therefore, the processing of photographs is considered processing of special categories of personal data when it involves the use of specific technical means, such as facial recognition, that allow or confirm the unique identification or authentication of a natural person3.Reference:1: Recital 51 of the GDPR2: Article 4(14) of the GDPR3: GDPR, Photographs, and Special Categories of Personal Data.