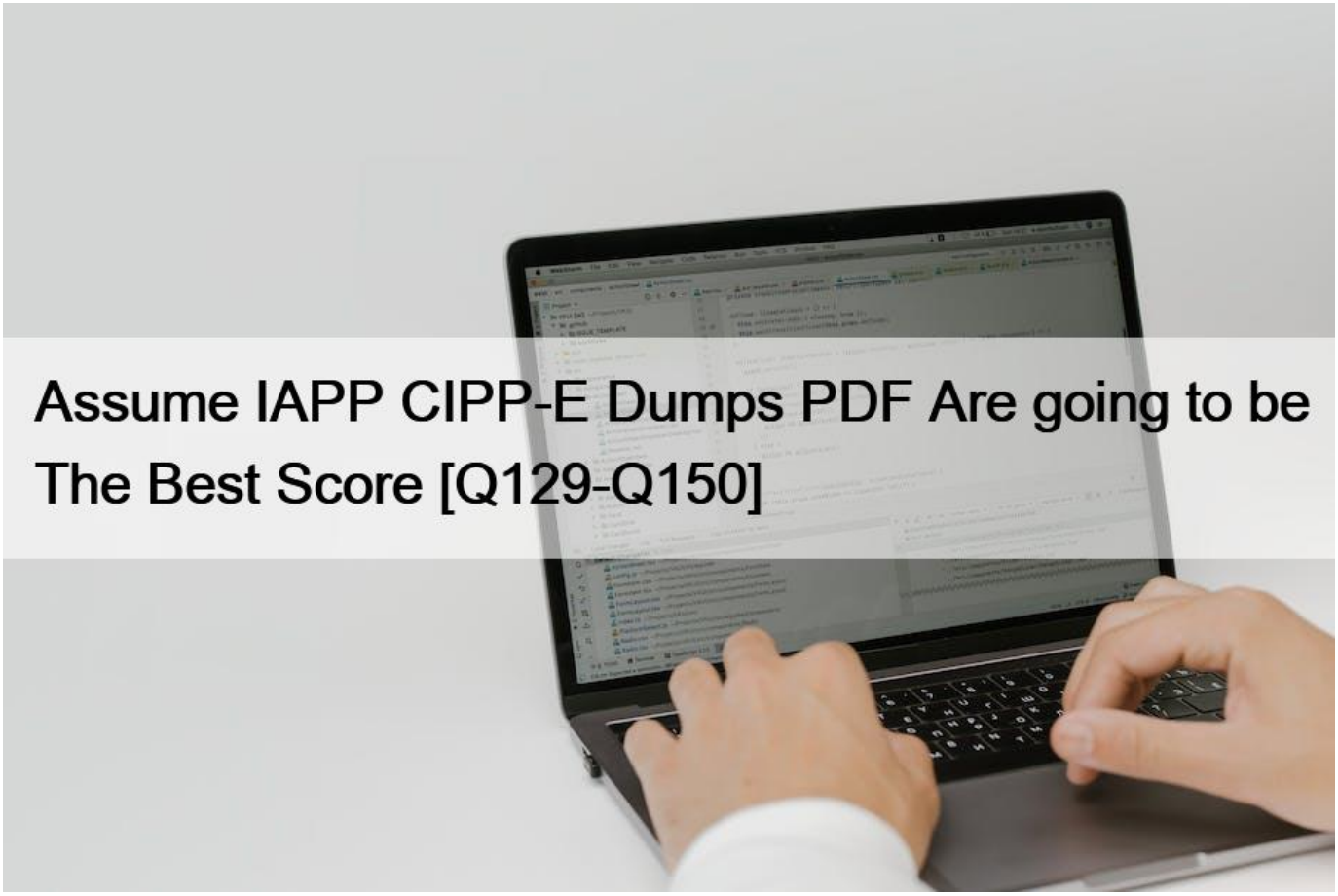
Assume IAPP CIPP-E Dumps PDF Are going to be The Best Score [Q129-Q150



Assume IAPP CIPP-E Dumps PDF Are going to be The Best Score
Certified Information Privacy Professional CIPP-E Exam and Certification Test Engine

QUESTION 129

What obligation does a data controller or processor have after appointing a data protection officer?
* To ensure that the data protection officer receives sufficient instructions regarding the exercise of his or her defined tasks.
* To provide resources necessary to carry out the defined tasks of the data protection officer and to maintain his or her expert knowledge.
* To ensure that the data protection officer acts as the sole point of contact for individuals’ Questions: about their personal data.
* To submit for approval to the data protection officer a code of conduct to govern organizational practices and demonstrate compliance with data protection principles.
Reference https://www.i-scoop.eu/gdpr/data-controller-data-controller-duties/

QUESTION 130

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

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

Section: (none)

Explanation

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

QUESTION 131

Which statement is correct when considering the right to privacy under Article 8 of the European Convention on Human Rights (ECHR)?

* The right to privacy is an absolute right
* The right to privacy has to be balanced against other rights under the ECHR
* The right to freedom of expression under Article 10 of the ECHR will always override the right to privacy
* The right to privacy protects the right to hold opinions and to receive and impart ideas without interference

Reference https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (15)

QUESTION 132

How is the retention of communications traffic data for law enforcement purposes addressed by European data protection law?

* The ePrivacy Directive allows individual EU member states to engage in such data retention.
* The ePrivacy Directive harmonizes EU member states’ rules concerning such data retention.
* The Data Retention Directive’s annulment makes such data retention now permissible.
* The GDPR allows the retention of such data for the prevention, investigation, detection or prosecution of criminal offences only.

The ePrivacy Directive is a European Union (EU) directive that aims to protect the confidentiality of electronic communications and prevent their indiscriminate interception or monitoring. It was adopted in 2002 and amended in 2009. It applies to all providers of electronic communication services, such as internet service providers, mobile network operators, and online platforms12.

One of the main objectives of the ePrivacy Directive is to ensure that the retention of communications traffic data for law enforcement purposes is subject to strict conditions and safeguards. Communications traffic data refers to any information relating to the transmission or routing of electronic communications, such as IP addresses, timestamps, and metadata3. Such data can be used by competent national authorities for the prevention, investigation, detection or prosecution of criminal offences and safeguarding national security4.

However, the ePrivacy Directive does not allow individual EU member states to engage in such data retention without harmonizing their rules. Article 6(1)(b) of the directive states that “Member States shall ensure that any measures taken by them in relation to the retention of traffic data are consistent with this Directive”. Therefore, each EU member state must adopt a national law that complies with the requirements and limitations set by the directive12.

The Data Retention Directive (DRD) was a previous EU directive that aimed to establish a common framework for the retention of communications traffic data for law enforcement purposes across all EU member states. It was adopted in 2006 and amended in 2010. However, it was annulled by the Court of Justice of the European Union (CJEU) in 2014 on procedural grounds. The CJEU found that some provisions of the DRD were inconsistent with other EU directives and principles, such as Article 8(2) of the Charter of Fundamental Rights (CFR), which protects individuals from arbitrary interference with their privacy56.

The GDPR is a new EU regulation that implements some aspects of the DRD into national law through its provisions on processing

personal data. However, it does not address directly the issue of communications traffic data retention for law enforcement purposes. Instead, it requires providers to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved in processing personal data. These measures include encryption, pseudonymisation, access control, and accountability7 . The GDPR also grants individuals certain rights regarding their personal data, such as access, rectification, erasure, portability, and objection7 .

Therefore, under current EU law, there is no single legal basis for retaining communications traffic data for law enforcement purposes across all EU member states. Each member state must adopt its own national law that respects the principles and limitations established by the ePrivacy Directive.

Reference:

ePrivacy Directive

ePrivacy Regulation

What is Communications Traffic Data?

How is Communications Traffic Data Retained?

Data Retention Directive

Data Retention Directive annulled by CJEU

General Data Protection Regulation

What are your rights regarding your personal data?

QUESTION 133

MagicClean is a web-based service located in the United States that matches home cleaning services to customers. It otters its services exclusively in the United States It uses a processor located in France to optimize its dat a. Is MagicClean subject to the GDPR?

* Yes, because MagicClean is processing data in the EU
* Yes. because MagicClean’s data processing agreement with the French processor is an establishment in the EU
* No, because MagicClean is located m the United States only.
* No. because MagicClean is not offering services to EU data subjects.

According to Article 3 of the GDPR, the regulation applies to the 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 regulation 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 such data subjects in the EU or the monitoring of their behaviour as far as their behaviour takes place within the EU. In this case, MagicClean is a controller not established in the EU, and it does not offer services to EU data subjects or monitor their behaviour. Therefore, MagicClean is not subject to the GDPR, even if it uses a processor located in France to optimize its data. The location of the processor does not determine the applicability of the GDPR, but the context of the activities of the controller or the processor and the relationship with the data subjects. Reference:

Article 3 of the GDPR

IAPP CIPP/E Study Guide, page 14

QUESTION 134

SCENARIO

Please use the following to answer the next question:

T-Craze, a German-headquartered specialty t-shirt company, was successfully selling to large German metropolitan cities. However, after a recent merger with another German-based company that was selling to a broader European market, T-Craze revamped its marketing efforts to sell to a wider audience. These efforts included a complete redesign of its logo to reflect the recent merger, and improvements to its website meant to capture more information about visitors through the use of cookies.

T-Craze also opened various office locations throughout Europe to help expand its business. While Germany continued to host T-Craze’s headquarters and main product-design office, its French affiliate became responsible for all marketing and sales activities. The French affiliate recently procured the services of Right Target, a renowned marketing firm based in the Philippines, to run its latest marketing campaign. After thorough research, Right Target determined that T-Craze is most successful with customers between the ages of 18 and 22. Thus, its first campaign targeted university students in several European capitals, which yielded nearly 40% new customers for T-Craze in one quarter. Right Target also ran subsequent campaigns for T- Craze, though with much less success.

The last two campaigns included a wider demographic group and resulted in countless unsubscribe requests, including a large number in Spain. In fact, the Spanish data protection authority received a complaint from Sofia, a mid-career investment banker. Sofia was upset after receiving a marketing communication even after unsubscribing from such communications from the Right Target on behalf of T-Craze.

Which of the following is T-Craze’s lead supervisory authority?
* Germany, because that is where T-Craze is headquartered.
* France, because that is where T-Craze conducts processing of personal information.
* Spain, because that is T-Craze’s primary market based on its marketing campaigns.
* T-Craze may choose its lead supervisory authority where any of its affiliates are based, because it has presence in several European countries.

QUESTION 135

SCENARIO

Please use the following to answer the next question:

ABC Hotel Chain and XYZ Travel Agency are U.S.-based multinational companies. They use an internet-based common platform for collecting and sharing their customer data with each other, in order to integrate their marketing efforts. Additionally, they agree on the data to be stored, how reservations will be booked and confirmed, and who has access to the stored data.

Mike, an EU resident, has booked travel itineraries in the past through XYZ Travel Agency to stay at ABC Hotel Chain’s locations. XYZ Travel Agency offers a rewards program that allows customers to sign up to accumulate points that can later be redeemed for free travel. Mike has signed the agreement to be a rewards program member.

Now Mike wants to know what personal information the company holds about him. He sends an email requesting access to his data, in order to exercise what he believes are his data subject rights.

What are ABC Hotel Chain and XYZ Travel Agency’s roles in this relationship?

* ABC Hotel Chain is the controller and XYZ Travel Agency is the processor.
* XYZ Travel Agency is the controller and ABC Hotel Chain is the processor.
* ABC Hotel Chain and XYZ Travel Agency are independent controllers.
* ABC Hotel Chain and XYZ Travel Agency are joint controllers.

QUESTION 136

According to the GDPR, what is the main task of a Data Protection Officer (DPO)?
* To create and maintain records of processing activities.
* To conduct Privacy Impact Assessments on behalf of the controller or processor.
* To monitor compliance with other local or European data protection provisions.
* To create procedures for notification of personal data breaches to competent supervisory authorities.

Reference https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required- gdpr-compliance

QUESTION 137

After leaving the EU under the terms of Brexit, the United Kingdom will seek an adequacy determination. What is the reason for this?
* The Insurance Commissioner determined that an adequacy determination is required by the Data Protection Act.
* Adequacy determinations automatically lapse when a Member State leaves the EU.
* The UK is now a third country because it’s no longer subject to the GDPR.
* The UK is less trustworthy now that its not part of the Union.

The GDPR applies to the 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 such data subjects in the EU or the monitoring of their behaviour as far as their behaviour takes place within the EU1. Therefore, after leaving the EU under the terms of Brexit, the UK became a third country for the purposes of the GDPR, meaning that personal data transfers from the EU to the UK are subject to the rules on international data transfers under Chapter V of the GDPR2. In order to ensure the continuity and stability of data flows between the EU and the UK, the UK sought an adequacy decision from the European Commission, which is a formal recognition that a third country provides an equivalent level of data protection to that of the EU3. On 28 June 2021, the European Commission adopted two adequacy decisions in respect of the UK: one for transfers under the GDPR and the other for transfers under the Law Enforcement Directive (LED)4. These decisions allow personal data to flow freely from the EU to the UK without any further safeguard being necessary, and are expected to last until 27 June 2025, unless they are amended, suspended or repealed earlier5. Reference:

GDPR, Article 3

GDPR, Chapter V

Data protection adequacy for non-EU countries, section “Adequacy decisions” UK government welcomes the European Commission’s draft data adequacy decisions Adequacy, section “What does the EU GDPR adequacy decision say?”

QUESTION 138

According to Article 14 of the GDPR, how long does a controller have to provide a data subject with necessary privacy information, if that subject’s personal data has been obtained from other sources?
* As soon as possible after obtaining the personal data.
* As soon as possible after the first communication with the data subject.
* Within a reasonable period after obtaining the personal data, but no later than one month.

* Within a reasonable period after obtaining the personal data, but no later than eight weeks.

QUESTION 139

In which case would a controller who has undertaken a DPIA most likely need to consult with a supervisory authority?
* Where the DPIA identifies that personal data needs to be transferred to other countries outside of the EEA.
* Where the DPIA identifies high risks to individuals’ rights and freedoms that the controller can take steps to reduce.
* Where the DPIA identifies that the processing being proposed collects the sensitive data of EU citizens.
* Where the DPIA identifies risks that will require insurance for protecting its business interests.

QUESTION 140

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.

Which of the following BEST describes the relationship between Liem, EcoMick and JaphSoft?
* Liem is a controller and EcoMick is a processor because Liem provides specific instructions regarding how the marketing campaigns should be rolled out.
* EcoMick and JaphSoft are is a controller and Liem is a processor because EcoMick is sharing its marketing data with Liem for contacts in Europe.
* JaphSoft is the sole processor because it processes personal data on behalf of its clients.
* Liem and EcoMick are joint controllers because they carry out joint marketing activities.

QUESTION 141

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?
* The AWS servers are located in the EU but in a country different than the location of the corporate headquarters.
* It is unlawful to process any personal data in a cloud unless the cloud is certified as GOPR-compliant by a competent supervisory authority.
* The data storage period has to be revised, and a data processing agreement w*h AWS must be signed
* 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.

QUESTION 142

Which institution has the power to adopt findings that confirm the adequacy of the data protection level in a non-EU country?
* The European Parliament
* The European Commission
* The Article 29 Working Party
* The European Council

QUESTION 143

Which marketing-related activity is least likely to be covered by the provisions of Privacy and Electronic Communications Regulations (Directive 2002/58/EC)?
* Advertisements passively displayed on a website.
* The use of cookies to collect data about an individual.
* A text message to individuals from a company offering concert tickets for sale.
* An email from a retail outlet promoting a sale to one of their previous customer.
Reference https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02002L0058- 20091219&from=RO

QUESTION 144

An unforeseen power outage results in company Z’s lack of access to customer data for six hours. According to article 32 of the GDPR, this is considered a breach. Based on the WP 29’s February, 2018 guidance, company Z should do which of the following?
* Notify affected individuals that their data was unavailable for a period of time.
* Document the loss of availability to demonstrate accountability

* Notify the supervisory authority about the loss of availability
* Conduct a thorough audit of all security systems

QUESTION 145

Read the following steps:

Discover which employees are accessing cloud services and from which devices and apps Lock down the data in those apps and devices Monitor and analyze the apps and devices for compliance Manage application life cycles Monitor data sharing An organization should perform these steps to do which of the following?
* Pursue a GDPR-compliant Privacy by Design process.
* Institute a GDPR-compliant employee monitoring process.
* Maintain a secure Bring Your Own Device (BYOD) program.
* Ensure cloud vendors are complying with internal data use policies.

The steps listed in the question are part of a best practice framework for implementing a secure BYOD program, which allows employees to use their personal devices to access organizational data and applications. A BYOD program poses significant privacy and security risks, such as data leakage, unauthorized access, malware infection, and compliance violations. Therefore, an organization should follow a comprehensive approach to discover, monitor, manage, and secure the devices, apps, and data involved in a BYOD program. This approach can help the organization meet the GDPR requirements for data protection by design and by default, data security, accountability, and data breach notification. Reference:

Free CIPP/E Study Guide, page 15, section 2.3.3

CIPP/E Certification, page 10, section 1.1.2

Cipp-e Study guides, Class notes & Summaries, document “CIPP/E Exam Summary 2023”, page 42, section 2.3.3

QUESTION 146

What must a data controller do in order to make personal data pseudonymous?
* Separately hold any information that would allow linking the data to the data subject.
* Encrypt the data in order to prevent any unauthorized access or modification.
* Remove all indirect data identifiers and dispose of them securely.
* Use the data only in aggregated form for research purposes.

Pseudonymisation is a method that allows you to switch the original data set (for example, e-mail or a name) with an alias or pseudonym, or, in other words, a value which does not allow the individual to be directly identified1. It is a reversible process that de-identifies data but allows the re-identification later on if necessary1. This is a well-known data management technique highly recommended by the General Data Protection Regulation (GDPR) as one of the data protection methods2. To make personal data pseudonymous, a data controller must separately hold any information that would allow linking the data to the data subject, such as a key or a code, and ensure that this information is kept securely and subject to technical and organisational measures to prevent unauthorised access or re-identification23. The other options are not correct, as they either describe other data protection methods, such as encryption or anonymisation, or do not meet the definition of pseudonymisation under the GDPR. Reference: Pseudonymization according to the GDPR, Pseudonymisation – Wikipedia, Anonymisation and pseudonymisation | Data Protection Commissioner

QUESTION 147

A company in France suffers a robbery over the weekend owing to a faulty alarm system. When it is determined that the break-in involves the loss of a substantial amount of data, the company decides on a CCTV system to monitor for future incidents. Company technicians install cameras in the entrance of the building, hallways and offices. Footage is recorded continuously, and is monitored

by the home office in the United States. What is the most realistic step the company could take to address their security concerns and comply with the personal data processing principles set out in Article 5 of the GDPR?
* Seek informed consent from company employees.
* Have cameras recording during work hours only.
* Retain captured footage for no more than 30 days.
* Restrict camera placement to building entrances only.

According to Article 5 of the GDPR, personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)1. The company’s decision to install cameras in the entrance of the building, hallways and offices may violate this principle, as it may expose the personal data of the employees and visitors to unnecessary risks, such as hacking, misuse or disclosure. Moreover, the company must also comply with the other principles of data processing, such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy and storage limitation1. The company must have a legitimate and specific purpose for installing the cameras, and must inform the data subjects about the processing of their personal data. The company must also ensure that the cameras collect only the minimum amount of data necessary for the purpose, and that the data are accurate and kept for no longer than necessary. The company must also respect the rights and freedoms of the data subjects, and provide them with the means to exercise their rights, such as the right to access, rectify, erase, restrict, object or port2.

The most realistic step the company could take to address their security concerns and comply with the personal data processing principles set out in Article 5 of the GDPR is to restrict the camera placement to building entrances only. This would limit the scope and impact of the data processing, and reduce the risks to the personal data of the employees and visitors. The company would still need to inform the data subjects about the processing, and ensure that the footage is securely stored and transferred, especially if it is monitored by the home office in the United States, which is a third country that may not offer adequate protection for personal data3. The company would also need to consider the possibility of obtaining the consent of the data subjects, or relying on another legal basis for the processing, such as the legitimate interests of the company or the performance of a contract4. Reference:

Article 5 of the GDPR

[Article 12-23 of the GDPR]

[Article 44-50 of the GDPR]

[Article 6 of the GDPR]

QUESTION 148

Read the following steps:

Discover which employees are accessing cloud services and from which devices and apps Lock down the data in those apps and devices Monitor and analyze the apps and devices for compliance Manage application life cycles Monitor data sharing An organization should perform these steps to do which of the following?
* Pursue a GDPR-compliant Privacy by Design process.
* Institute a GDPR-compliant employee monitoring process.
* Maintain a secure Bring Your Own Device (BYOD) program.
* Ensure cloud vendors are complying with internal data use policies.

Reference https://www.itproportal.com/features/heading-off-the-spectre-of-gdpr-compliance-with-secure-byod/

QUESTION 149

Please use the following to answer the next question:

ProStorage is a multinational cloud storage provider headquartered in the Netherlands. Its CEO. Ruth Brown, has developed a two-pronged strategy for growth: 1) expand ProStorage s global customer base and 2) increase ProStorage’s sales force by efficiently onboarding effective teams. Enacting this strategy has recently been complicated by Ruth’s health condition, which has limited her working hours, as well as her ability to travel to meet potential customers. ProStorage’s Human Resources department and Ruth’s Chief of Staff now work together to manage her schedule and ensure that she is able to make all her medical appointments The latter has become especially crucial after Ruth’s last trip to India, where she suffered a medical emergency and was hospitalized m New Delhi Unable to reach Ruths family, the hospital reached out to ProStorage and was able to connect with her Chief of Staff, who in coordination with Mary, the head of HR. provided information to the doctors based on accommodate on requests Ruth made when she started a: ProStorage Why is the additional measure recommended by Jackie sufficient foe using UpFinance?

* UpFinance is an established 7-year-old business.
* UpFinance is in a highly regulated financial industry
* UpFinance is based in a country without surveillance laws.
* UpFinance implements sufficient data protection measures

QUESTION 150

SCENARIO

Please use the following to answer the next question:

T-Craze, a German-headquartered specialty t-shirt company, was successfully selling to large German metropolitan cities. However, after a recent merger with another German-based company that was selling to a broader European market, T-Craze revamped its marketing efforts to sell to a wider audience. These efforts included a complete redesign of its logo to reflect the recent merger, and improvements to its website meant to capture more information about visitors through the use of cookies.

T-Craze also opened various office locations throughout Europe to help expand its business. While Germany continued to host T-Craze’s headquarters and main product-design office, its French affiliate became responsible for all marketing and sales activities. The French affiliate recently procured the services of Right Target, a renowned marketing firm based in the Philippines, to run its latest marketing campaign. After thorough research, Right Target determined that T-Craze is most successful with customers between the ages of 18 and 22. Thus, its first campaign targeted university students in several European capitals, which yielded nearly 40% new customers for T-Craze in one quarter. Right Target also ran subsequent campaigns for T- Craze, though with much less success.

The last two campaigns included a wider demographic group and resulted in countless unsubscribe requests, including a large number in Spain. In fact, the Spanish data protection authority received a complaint from Sofia, a mid-career investment banker. Sofia was upset after receiving a marketing communication even after unsubscribing from such communications from the Right Target on behalf of T-Craze.

Which of the following is T-Craze’s lead supervisory authority?

* Germany, because that is where T-Craze is headquartered.
* France, because that is where T-Craze conducts processing of personal information.
* Spain, because that is T-Craze’s primary market based on its marketing campaigns.
* T-Craze may choose its lead supervisory authority where any of its affiliates are based, because it has presence in several European countries.

Use CIPP-E Exam Dumps (2024 PDF Dumps) To Have Reliable CIPP-E Test Engine:
https://www.examslabs.com/IAPP/Certified-Information-Privacy-Professional/best-CIPP-E-exam-dumps.html]