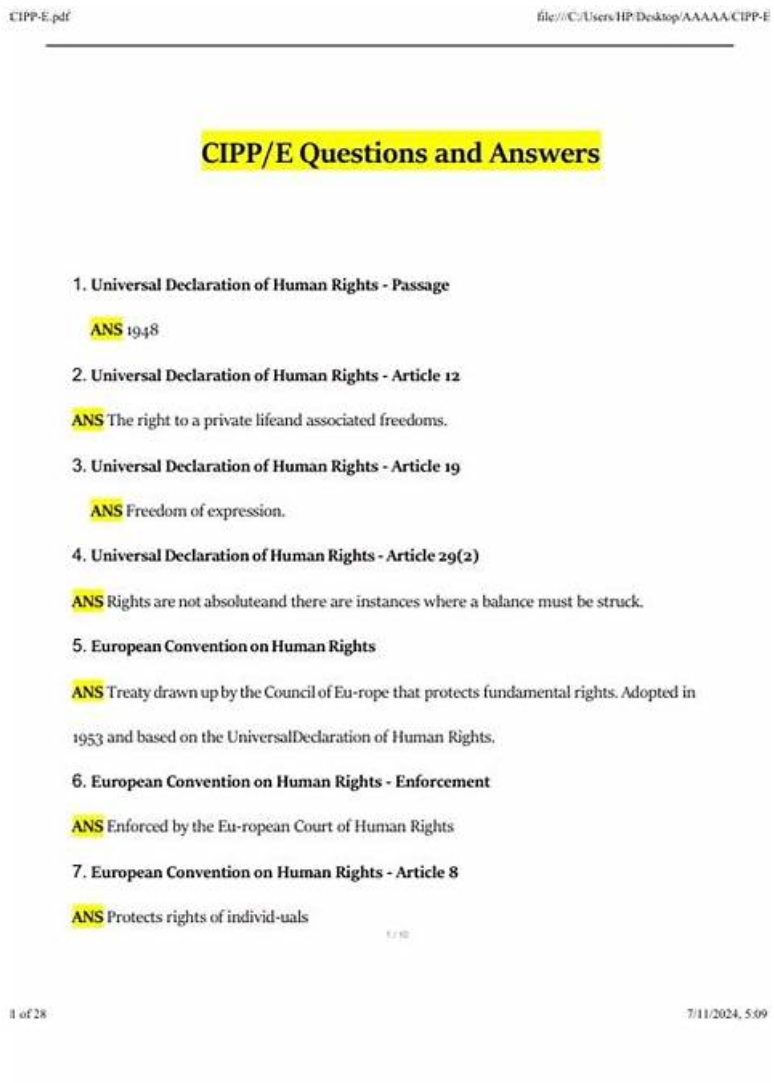
New CIPP-E Braindumps Files, CIPP-E PDF Questions



CIPP-E.pdf file:///C:/Users/HP/Desktop/AAAAA/CIPP-E

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 lifeand 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 absoluteand there are instances where a balance must be struck.

5. **European Convention on Human Rights**

ANS Treaty drawn up by the Council of Eu-rope that protects fundamental rights. Adopted in 1953 and based on the UniversalDeclaration of Human Rights.

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

ANS Enforced by the Eu-ropean Court of Human Rights

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

ANS Protects rights of individ-uals

1 of 28 7/11/2024, 5:09

What's more, part of that PrepAwayTest CIPP-E dumps now are free: https://drive.google.com/open?id=1bLY0ZOAncsYM6GDoxiuBu6zOtDs4H1Dl

The Certified Information Privacy Professional/Europe (CIPP/E) (CIPP-E) practice questions (desktop and web-based) are customizable, meaning users can set the questions and time according to their needs to improve their discipline and feel the real-based exam scenario to pass the IAPP CIPP-E Certification. Customizable mock tests comprehensively and accurately represent the actual IAPP CIPP-E certification exam scenario.

The CIPP/E certification exam is offered by the International Association of Privacy Professionals (IAPP), the world's largest association of privacy professionals. The IAPP is committed to advancing the privacy profession by providing education, networking opportunities, and certification programs. The CIPP/E certification is one of four certifications offered by the IAPP, with the others being CIPP/US, CIPM, and CIPT.

>> New CIPP-E Braindumps Files <<

CIPP-E PDF Questions - Pass CIPP-E Rate

Because customer first, service first is our principle of service. If you buy our CIPP-E study guide, you will find our after sale service is so considerate for you. We are glad to meet your all demands and answer your all question about our CIPP-E study materials. We can make sure that if you purchase our CIPP-E Exam Questions, you will have the right to enjoy our perfect after sale service and the high quality products. So do not hesitate and buy our CIPP-E study guide, we believe you will find surprise from our CIPP-

E exam questions.

IAPP CIPP-E (Certified Information Privacy Professional/Europe) exam is a certification program designed to test an individual's knowledge on data privacy laws and regulations in the European Union (EU). Certified Information Privacy Professional/Europe (CIPP/E) certification is internationally recognized and is highly valued by employers in the EU and beyond. The CIPP-E Exam is administered by the International Association of Privacy Professionals (IAPP), a leading organization in the field of privacy and data protection.

IAPP Certified Information Privacy Professional/Europe (CIPP/E) Sample Questions (Q55-Q60):

NEW QUESTION # 55
SCENARIO
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 In support of Ruth's strategic goals of hiring more sales representatives, the Human Resources team is focused on improving its processes to ensure that new employees are sourced, interviewed, hired, and onboarded efficiently. To help with this, Mary identified two vendors, HRYourWay, a German based company, and InstaHR, an Australian based company. She decided to have both vendors go through ProStorage's vendor risk review process so she can work with Ruth to make the final decision. As part of the review process, Jackie, who is responsible for maintaining ProStorage's privacy program (including maintaining controller BCRs and conducting vendor risk assessments), reviewed both vendors but completed a transfer impact assessment only for InstaHR. After her review of both boasted a more established privacy program and provided third-party attestations, whereas HRYourWay was a small vendor with minimal data protection operations.
Thus, she recommended InstaHR.
ProStorage's marketing team also worked to meet the strategic goals of the company by focusing on industries where it needed to grow its market share. To help with this, the team selected as a partner UpFinance, a US based company with deep connections to financial industry customers. During ProStorage's diligence process, Jackie from the privacy team noted in the transfer impact assessment that UpFinance implements several data protection measures including end-to-end encryption, with encryption keys held by the customer.
Notably, UpFinance has not received any government requests in its 7 years of business. Still, Jackie recommended that the contract require UpFinance to notify ProStorage if it receives a government request for personal data UpFinance processes on its behalf prior to disclosing such data.
What transfer mechanism should Jackie recommend for using InstaHR?

- A. Explicit consent of employees.
- B. Adequacy
- C. Binding corporate rules.
- D. Standard contractual clauses

Answer: D

Explanation:
According to the GDPR, any transfer of personal data to a third country or an international organisation must be based on an adequacy decision by the Commission, appropriate safeguards by the data exporter and importer, or derogations for specific situations1. In this scenario, InstaHR is an Australian based company that processes personal data on behalf of ProStorage, a Dutch based company. Australia is not recognised by the Commission as a country that provides an adequate level of data protection2, so the adequacy option is not available. Binding corporate rules (BCRs) are internal rules adopted by multinational groups of companies or organisations that define their global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries that do not provide an adequate level of protection3. However, BCRs are not applicable in this case, as InstaHR is not part of the same corporate group as ProStorage. Explicit consent of employees is a possible derogation for specific situations, but it is not a reliable or practical transfer mechanism, as it must be freely given, specific, informed and unambiguous, and it can be withdrawn at any time4. Therefore, the most suitable transfer mechanism for using InstaHR is standard contractual clauses (SCCs). SCCs are contractual clauses that have been pre-approved by the Commission and that provide appropriate safeguards for data protection when transferring personal data from the EU/EEA to third countries. SCCs are legally

binding and enforceable by data subjects, and they impose obligations on both the data exporter and the data importer. SCCs are widely used by data controllers and processors as a transfer mechanism under the GDPR. Reference: 1: Art. 44 GDPR - General principle for transfers22: Adequacy decisions - European Commission13: Binding corporate rules - European Commission14: Article 7 of the GDPR. : Standard Contractual Clauses (SCC) - European Commission1.

NEW QUESTION # 56
What is the key difference between the European Council and the Council of the European Union?

- A. The European Council focuses primarily on issues involving human rights.
- B. The Council of the European Union has a degree of legislative power.
- C. The Council of the European Union is helmed by a president.
- D. The European Council is comprised of the heads of each EU member state.

Answer: D

Explanation:
The European Council and the Council of the European Union are two different EU institutions that have similar names but distinct roles and memberships. The European Council is the body of leaders (heads of state or government) of the 27 EU member states that defines the EU's general political direction and priorities1. The European Council does not adopt EU legislation, but rather sets the agenda and gives guidance to the other EU institutions1. The Council of the European Union, informally known as the Council, is composed of national ministers from each EU member state, grouped by policy area1. The Council is one of the two legislative bodies of the EU, along with the European Parliament, and negotiates and adopts EU laws, coordinates member states' policies, and develops the EU's common foreign and security policy1. The key difference between the two institutions is that the European Council is comprised of the heads of each EU member state, while the Council of the European Union is comprised of the ministers of each EU member state12. References: European Council | Council of the European Union, What is the difference between EU Council, Council of the European Union, and Council of Europe?

NEW QUESTION # 57
What monitoring may lawfully be performed within the scope of Gentle Hedgehog's business?

- A. Only emails, website browsing history, and camera for internal video calls that are expressly marked as monitored.
- B. Everything offered by Sauron Eye's software in relation to activity by sales team contractors.
- C. Only emails, website browsing history, and camera for internal video calls conducted in a non-secure environment.
- D. Everything offered by Sauron Eye's software, assuming employees provide daily consent to the monitoring.

Answer: A

Explanation:
Under GDPR and EU employment law, employee monitoring must comply with the principles of necessity, proportionality, legitimacy, and transparency.
* Legal requirements for employee monitoring:
* Necessity: Employers must demonstrate that monitoring is necessary for a legitimate purpose.
* Proportionality: The monitoring must be the least intrusive method available.
* Transparency: Employees must be fully informed about what is being monitored.
* Why is D the correct answer?
* GDPR requires that monitoring must be explicitly communicated and justified.
* Employers can monitor work emails, browsing history, and video calls, but only if employees are clearly informed and the purpose is justified.
* Why are other answers incorrect?
* A (Monitoring all contractor activity) # Contractors have data protection rights too; monitoring must still be necessary and proportionate.
* B (Daily consent requirement) # Employee consent is not valid under GDPR in most cases due to power imbalance.
* C (Monitoring in non-secure environments only) # The location does not determine the lawfulness of monitoring.
Conclusion: The correct answer is D, as only explicitly marked and justified monitoring is lawful under GDPR.

NEW QUESTION # 58
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 establishment of a list of legitimate data processing criteria
- B. The synchronization of approaches to data protection
- C. The creation of legally binding data protection principles
- D. The restriction of cross-border data flow

Answer: B

NEW QUESTION # 59
SCENARIO
Please use the following to answer the next question:
Due to rapidly expanding workforce, Company A has decided to outsource its payroll function to Company B.
Company B is an established payroll service provider with a sizable client base and a solid reputation in the industry.
Company B's payroll solution for Company A relies on the collection of time and attendance data obtained via a biometric entry system installed in each of Company A's factories. Company B won't hold any biometric data itself, but the related data will be uploaded to Company B's UK servers and used to provide the payroll service. Company B's live systems will contain the following information for each of Company A's employees:
* Name
* Address
* Date of Birth
* Payroll number
* National Insurance number
* Sick pay entitlement
* Maternity/paternity pay entitlement
* Holiday entitlement
* Pension and benefits contributions
* Trade union contributions
Jenny is the compliance officer at Company A. She first considers whether Company A needs to carry out a data protection impact assessment in relation to the new time and attendance system, but isn't sure whether or not this is required.
Jenny does know, however, that under the GDPR there must be a formal written agreement requiring Company B to use the time and attendance data only for the purpose of providing the payroll service, and to apply appropriate technical and organizational security measures for safeguarding the data. Jenny suggests that Company B obtain advice from its data protection officer. The company doesn't have a DPO but agrees, in the interest of finalizing the contract, to sign up for the provisions in full. Company A enters into the contract.
Weeks later, while still under contract with Company A, Company B embarks upon a separate project meant to enhance the functionality of its payroll service, and engages Company C to help. Company C agrees to extract all personal data from Company B's live systems in order to create a new database for Company B.
This database will be stored in a test environment hosted on Company C's U.S. server. The two companies agree not to include any data processing provisions in their services agreement, as data is only being used for IT testing purposes.
Unfortunately, Company C's U.S. server is only protected by an outdated IT security system, and suffers a cyber security incident soon after Company C begins work on the project. As a result, data relating to Company A's employees is visible to anyone visiting Company C's website. Company A is unaware of this until Jenny receives a letter from the supervisory authority in connection with the investigation that ensues.
As soon as Jenny is made aware of the breach, she notifies all affected employees.
Under the GDPR, which of Company B's actions would NOT be likely to trigger a potential enforcement action?

- A. Their omission of data protection provisions in their contract with Company C.
- B. Their failure to provide sufficient security safeguards to Company A's data.
- C. Their engagement of Company C to improve their payroll service.
- D. Their decision to operate without a data protection officer.

Answer: C

Explanation:
While Company B made several mistakes in handling Company A's employee data, not all of them would likely trigger a potential enforcement action under the GDPR. Here's an analysis of each option:
A: Omission of data protection provisions in the contract with Company C: This is a clear violation of the GDPR. Company B, as the data controller, is responsible for ensuring that any third-party processors comply with data protection requirements. By omitting data protection provisions in the contract, Company B failed to take appropriate steps to ensure the security and privacy of the

personal data. This would be a likely trigger for an enforcement action.
B: Failure to provide sufficient security safeguards to Company A's data: This is another violation of the GDPR. Company B has a legal obligation to implement appropriate technical and organizational security measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction. The outdated IT security system at Company C's U.S. server demonstrates a failure to meet this obligation. This would also be a likely trigger for an enforcement action.
C: Engagement of Company C to improve their payroll service: While outsourcing certain aspects of data processing is permitted under the GDPR, the data controller remains ultimately responsible for compliance.
However, simply engaging another company to improve a service itself isn't necessarily a violation. As long as the proper safeguards are in place and the data processing is carried out in accordance with the GDPR, this action alone would not likely trigger an enforcement action.
D: Decision to operate without a data protection officer: The GDPR requires certain organizations to appoint a data protection officer (DPO). While Company B may be required to have a DPO depending on its size and activities, the absence of a DPO wouldn't automatically trigger an enforcement action. However, it could indicate a lack of compliance culture and contribute to other violations, increasing the likelihood of an enforcement action.
Therefore, while Company B made several mistakes, only the ones that directly violate specific data protection requirements, such as omitting data protection provisions in contracts or failing to implement appropriate security measures, are likely to trigger an enforcement action. Engaging a third-party to improve a service, as long as it's done in a compliant manner, isn't a violation in itself.

NEW QUESTION # 60
......

CIPP-E PDF Questions: https://www.prepawaytest.com/IAPP/CIPP-E-practice-exam-dumps.html

id=1bLY0ZOAncsYM6GDoxiuBu6zOtDs4H1Dl