CIPP-E Training & Certification Get Latest Certified Information Privacy Professional Updated on Feb 07, 2024 [Q98-Q113

CIPP-E Training & Certification Get Latest Certified Information Privacy Professional Updated on Feb 07, 2024
Certification Training for CIPP-E Exam Dumps Test Engine

What ways to study the IAPP Exam

There are two main types of resources for preparation of certification exams first there are the study guides and the books that are detailed and suitable for building knowledge from the ground up then there are video tutorial and lectures that can somehow ease the pain of through study and are comparatively less boring for some candidates yet these demand time and concentration from the learner. Smart Candidates who want to build a solid foundation in all exam topics and related technologies usually combine video lectures with study guides to reap the benefits of both but there is one crucial preparation tool as often overlooked by most candidates the practice exams. Practice exams are built to make students comfortable with the real exam environment. Statistics have shown that most students fail not due to that preparation but due to exam anxiety the fear of the unknown. VCEPrep expert team recommends you prepare some notes on these topics along with it don't forget to practice IAPP CIPP/E Exam exam dumps which been written by our expert team, Both these will help you a lot to clear this exam with good marks.

The IAPP CIPP-E exam is administered by the International Association of Privacy Professionals (IAPP), a non-profit organization dedicated to promoting privacy and data protection practices around the world. The IAPP CIPP-E exam is one of several

certification exams offered by the organization, including exams focused on privacy in other regions of the world, as well as exams for specific industries, such as healthcare or financial services.

Q98. What term BEST describes the European model for data protection?
* Sectoral
* Self-regulatory
* Market-based
* Comprehensive

Q99. What was the main failing of Convention 108 that led to the creation of the Data Protection Directive (Directive 95/46/EC)?
* IT did not account for the rapid growth of the Internet
* It did not include protections for sensitive personal data
* It was implemented in a fragmented manner by a small number of states.
* Its penalties for violations of data protection rights were widely viewed as r sufficient.

Q100. As a result of the European Court of Justice’s ruling in the case of Google v. Spain, search engines outside the EEA are also likely to be subject to the Regulation’s right to be forgotten. This holds true if the activities of an EU subsidiary and its U.S. parent are what?
* Supervised by the same Data Protection Officer.
* Consistent with Privacy Shield requirements
* Bound by a standard contractual clause.
* Inextricably linked in their businesses.

Q101. In the event of a data breach, which type of information are data controllers NOT required to provide to either the supervisory authorities or the data subjects?
* The predicted consequences of the breach.
* The measures being taken to address the breach.
* The type of security safeguards used to protect the data.
* The contact details of the appropriate data protection officer.

According to the CIPP/E study guide, Article 33 of the GDPR requires data controllers to notify the supervisory authority of a personal data breach without undue delay and, where feasible, not later than 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons1. Article 34 of the GDPR requires data controllers to communicate the personal data breach to the data subject without undue delay when the breach is likely to result in a high risk to the rights and freedoms of natural persons2. Both articles specify the minimum information that the data controller must provide to the supervisory authority and the data subject, which includes: the nature of the breach, the categories and approximate number of data subjects and personal data records concerned, the name and contact details of the data protection officer or other contact point, the likely consequences of the breach, and the measures taken or proposed to address the breach and mitigate its possible adverse effects12. However, neither article requires the data controller to disclose the type of security safeguards used to protect the data, as this information is not relevant for the purposes of notification and may even compromise the security of the data further3.
Reference: 1: CIPP/E study guide, page 84; Art. 33 GDPR; Guidelines 01/2021 on Examples regarding Data Breach Notification2: CIPP/E study guide, page 85; [Art. 34 GDPR]; Guidelines 01/2021 on Examples regarding Data Breach Notification3: Personal Data Breach | European Data Protection Supervisor; What is a data breach and what do we have to do … – European Commission.

Q102. When collecting personal data in a European Union (EU) member state, what must a company do if it collects personal data from a source other than the data subjects themselves?
* Inform the subjects about the collection
* Provide a public notice regarding the data
* Upgrade security to match that of the source

* Update the data within a reasonable timeframe

Q103. SCENARIO

Please use the following to answer the next question:

Joe started the Gummy Bear Company in 2000 from his home in Vermont, USA.

Today, it is a multi-billion-dollar candy company operating in every continent. All of the company’s IT servers are located in Vermont. This year Joe hires his son Ben to join the company and head up Project Big, which is a major marketing strategy to triple gross revenue in just 5 years. Ben graduated with a PhD in computer software from a top university. Ben decided to join his father’s company, but is also secretly working on launching a new global online dating website company called Ben Knows Best.

Ben is aware that the Gummy Bear Company has millions of customers and believes that many of them might also be interested in finding their perfect match. For Project Big, Ben redesigns the company’s online web portal and requires customers in the European Union and elsewhere to provide additional personal information in order to remain a customer. Project Ben begins collecting data about customers’ philosophical beliefs, political opinions and marital status.

If a customer identifies as single, Ben then copies all of that customer’s personal data onto a separate database for Ben Knows Best. Ben believes that he is not doing anything wrong, because he explicitly asks each customer to give their consent by requiring them to check a box before accepting their information. As Project Big is an important project, the company also hires a first year college student named Sam, who is studying computer science to help Ben out.

Ben calls out and Sam comes across the Ben Knows Best database. Sam is planning on going to Ireland over Spring Beak with 10 of his friends, so he copies all of the customer information of people that reside in Ireland so that he and his friends can contact people when they are in Ireland.

Joe also hires his best friend’s daughter, Alice, who just graduated from law school in the U.S., to be the company’s new General Counsel. Alice has heard about the GDPR, so she does some research on it. Alice approaches Joe and informs him that she has drafted up Binding Corporate Rules for everyone in the company to follow, as it is important for the company to have in place a legal mechanism to transfer data internally from the company’s operations in the European Union to the U.S.

Joe believes that Alice is doing a great job, and informs her that she will also be in-charge of handling a major lawsuit that has been brought against the company in federal court in the U.S. To prepare for the lawsuit, Alice instructs the company’s IT department to make copies of the computer hard drives from the entire global sales team, including the European Union, and send everything to her so that she can review everyone’s information. Alice believes that Joe will be happy that she did the first level review, as it will save the company a lot of money that would otherwise be paid to its outside law firm.

When Ben had the company collect additional data from its customers, the most serious violation of the GDPR occurred because the processing of the data created what?
* An information security risk by copying the data into a new database.
* A potential legal liability and financial exposure from its customers.
* A significant risk to the customers’ fundamental rights and freedoms.
* A significant risk due to the lack of an informed consent mechanism.

Q104. SCENARIO

Please use the following to answer the next question:

Brady is a computer programmer based in New Zealand who has been running his own business for two years. Brady’s business provides a low-cost suite of services to customers throughout the European Economic Area (EEA). The services are targeted towards new and aspiring small business owners. Brady’s company, called Brady Box, provides web page design services, a Social Networking Service (SNS) and consulting services that help people manage their own online stores.

Unfortunately, Brady has been receiving some complaints. A customer named Anna recently uploaded her plans for a new product onto Brady Box’s chat area, which is open to public viewing. Although she realized her mistake two weeks later and removed the document, Anna is holding Brady Box responsible for not noticing the error through regular monitoring of the website. Brady believes he should not be held liable.

Another customer, Felipe, was alarmed to discover that his personal information was transferred to a third- party contractor called Hermes Designs and worries that sensitive information regarding his business plans may be misused. Brady does not believe he violated European privacy rules. He provides a privacy notice to all of his customers explicitly stating that personal data may be transferred to specific third parties in fulfillment of a requested service. Felipe says he read the privacy notice but that it was long and complicated Brady continues to insist that Felipe has no need to be concerned, as he can personally vouch for the integrity of Hermes Designs. In fact, Hermes Designs has taken the initiative to create sample customized banner advertisements for customers like Felipe. Brady is happy to provide a link to the example banner ads, now posted on the Hermes Designs webpage. Hermes Designs plans on following up with direct marketing to these customers.

Brady was surprised when another customer, Serge, expressed his dismay that a quotation by him is being used within a graphic collage on Brady Box’s home webpage. The quotation is attributed to Serge by first and last name. Brady, however, was not worried about any sort of litigation. He wrote back to Serge to let him know that he found the quotation within Brady Box’s Social Networking Service (SNS), as Serge himself had posted the quotation. In his response, Brady did offer to remove the quotation as a courtesy.

Despite some customer complaints, Brady’s business is flourishing. He even supplements his income through online behavioral advertising (OBA) via a third-party ad network with whom he has set clearly defined roles. Brady is pleased that, although some customers are not explicitly aware of the OBA, the advertisements contain useful products and services.

Under the General Data Protection Regulation (GDPR), what is the most likely reason Serge may have grounds to object to the use of his quotation?
* Because of the misrepresentation of personal data as an endorsement.
* Because of the juxtaposition of the quotation with others’ quotations.
* Because of the use of personal data outside of the social networking service (SNS).
* Because of the misapplication of the household exception in relation to a social networking service (SNS).

Q105. SCENARIO

Please use the following to answer the next question:

Zandelay Fashion (‘Zandelay’) is a successful international online clothing retailer that employs approximately

650 people at its headquarters based in Dublin, Ireland. Martin is their recently appointed data protection officer, who oversees the company’s compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.

The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.

In an aggressive bid to build revenue growth, Jerry, the CEO, tells Martin that the company is launching a new mobile app and

loyalty scheme that puts significant emphasis on profiling the company’s customers by analyzing their purchases. Martin tells the CEO that: (a) the potential risks of such activities means that Zandelay needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures. Zandelay may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.

Jerry tells Martin that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Zandelay’s business plan and associated processing activities.

What must Zandelay provide to the supervisory authority during the prior consultation?
* An evaluation of the complexity of the intended processing.
* An explanation of the purposes and means of the intended processing.
* Records showing that customers have explicitly consented to the intended profiling activities.
* Certificates that prove Martin’s professional qualities and expert knowledge of data protection law.

Q106. 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?
* Their omission of data protection provisions in their contract with Company C.
* Their failure to provide sufficient security safeguards to Company A’s data.
* Their engagement of Company C to improve their payroll service.
* Their decision to operate without a data protection officer.

Q107. Please use the following to answer the next question:

Jack worked as a Pharmacovigiliance Operations Specialist in the Irish office of a multinational pharmaceutical company on a clinical trial related to COVID-19. As part of his onboarding process Jack received privacy training He was explicitly informed that while he would need to process confidential patient data in the course of his work, he may under no circumstances use this data for anything other than the performance of work-related (asks This was also specified in the privacy policy, which Jack signed upon conclusion of the training.

After several months of employment, Jack got into an argument with a patient over the phone. Out of anger he later posted the patient’s name and hearth information, along with disparaging comments, on a social media website. When this was discovered by his Pharmacovigilance supervisors. Jack was immediately dismissed Jack’s lawyer sent a letter to the company stating that dismissal was a disproportionate sanction, and that if Jack was not reinstated within 14 days his firm would have no alternative but to commence legal proceedings against the company. This letter was accompanied by a data access request from Jack requesting a copy of “all personal data, including internal emails that were sent/received by Jack or where Jack is directly or indirectly identifiable from the contents. In relation to the emails Jack listed six members of the management team whose inboxes the required access.

How should the company respond to Jack’s request to be forgotten?
* The company should not erase the data at this time as it may be required to defend a legal claim of unfair dismissal.
* The company should erase all data relating to Jack without undue delay as the right to be forgotten is an absolute right.
* The company should claim that the right to be forgotten is not applicable to them, as only a fraction of their global workforce resides in the European Union.

* The company should ensure that the information is stored outside of the European Union so that the right to be forgotten under the GDPR does not apply.

Q108. According to the GDPR, when should the processing of photographs be considered processing of special categories of personal data?
* When processed with the intent to publish information regarding a natural person on publicly accessible media.
* When processed with the intent to proceed to scientific or historical research projects.
* When processed with the intent to uniquely identify or authenticate a natural person.
* When processed with the intent to comply with a law.
Reference:

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.

Q109. A U.S. company’s website sells widgets. Which of the following factors would NOT in itself subject the company to the GDPR?
* The widgets are offered in EU and priced in euro.
* The website is in English and French, and is accessible in France.
* An affiliate office is located in France but the processing is in the U.S.
* The website places cookies to monitor the EU website user behavior.

Q110. SCENARIO

Please use the following to answer the next question:

Louis, a long-time customer of Bedrock Insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Louis has been plagued by texts and calls from a company called Accidentable offering to help him recover compensation for personal injury. Louis has heard about insurance companies selling customers’ data to third parties, and he’s convinced that Accidentable must have gotten his information from Bedrock Insurance.

Louis has also been receiving an increased amount of marketing information from Bedrock, trying to sell him their full range of their insurance policies.

Perturbed by this, Louis has started looking at price comparison sites on the internet and has been shocked to find that other insurers offer much cheaper rates than Bedrock, even though he has been a loyal customer for many years. When his Bedrock policy comes up for renewal, he decides to switch to Zantrum Insurance.

In order to activate his new insurance policy, Louis needs to supply Zantrum with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask Bedrock to transfer his information directly to Zantrum. He also takes this opportunity to ask Bedrock to stop using his personal data for marketing purposes.

Bedrock supplies Louis with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Louis it cannot transfer his data directly to Zantrum as this is not technically feasible. Bedrock also explains that Louis’s contract included a provision whereby Louis agreed that his data could be used for marketing purposes; according to Bedrock, it is too late

for Louis to change his mind about this. It angers Louis when he recalls the wording of the contract, which was filled with legal jargon and very confusing.

In the meantime, Louis is still receiving unwanted calls from Accidentable Insurance. He writes to Accidentable to ask for the name of the organization that supplied his details to them. He warns Accidentable that he plans to complain to the data protection authority, because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.

Accidentable’s response letter confirms Louis’s suspicions. Accidentable is Bedrock Insurance’s wholly owned subsidiary, and they received information about Louis’s accident from Bedrock shortly after Louis submitted his accident claim. Accidentable assures Louis that there has been no breach of the GDPR, as Louis’s contract included, a provision in which he agreed to share his information with Bedrock’s affiliates for business purposes.

Louis is disgusted by the way in which he has been treated by Bedrock, and writes to them insisting that all his information be erased from their computer system.

Which statement accurately summarizes Bedrock’s obligation in regard to Louis’s data portability request?
* Bedrock does not have a duty to transfer Louis’s data to Zantrum if doing so is legitimately not technically feasible.
* Bedrock does not have to transfer Louis’s data to Zantrum because the right to data portability does not apply where personal data are processed in order to carry out tasks in the public interest.
* Bedrock has failed to comply with the duty to transfer Louis’s data to Zantrum because the duty applies wherever personal data are processed by automated means and necessary for the performance of a contract with the customer.
* Bedrock has failed to comply with the duty to transfer Louis’s data to Zantrum because it has an obligation to develop commonly used, machine-readable and interoperable formats so that all customer data can be ported to other insurers on request.

Q111. Which of the following is the weakest lawful basis for processing employee personal data?
* Processing based on fulfilling an employment contract.
* Processing based on employee consent.
* Processing based on legitimate interests.
* Processing based on legal obligation.
Reference:

According to the GDPR, consent is one of the six lawful bases for processing personal data, but it is not always the most appropriate one. Consent must be freely given, specific, informed and unambiguous, and the data subject must have the right to withdraw it at any time1. In the context of employment, consent is often not a valid lawful basis, because there is a clear imbalance of power between the employer and the employee, which means that the consent is not freely given2. Moreover, consent can be difficult to manage and document, and it can pose practical problems if the employee withdraws it. Therefore, consent is the weakest lawful basis for processing employee personal data, and employers should rely on other lawful bases, such as contract, legal obligation, vital interests, public task or legitimate interests, depending on the purpose and necessity of the processing3. Reference: 1: Article 4(11) and Article 7 of the GDPR; 2: [EDPB Guidelines], page 6; 3: A Guide to Lawful Basis for Processing Employee Personal Data.

Q112. An entity’s website stores text files on EU users’ computer and mobile device browsers. Prior to doing so, the entity is required to provide users with notices containing information and consent under which of the following frameworks?
* General Data Protection Regulation 2016/679.
* E-Privacy Directive 2002/58/EC.
* E-Commerce Directive 2000/31/EC.
* Data Protection Directive 95/46/EC.

Q113. SCENARIO

Please use the following to answer the next question:

Financially, it has been a very good year at ARRA Hotels: Their 21 hotels, located in Greece (5), Italy (15) and Spain (1), have registered their most profitable results ever. To celebrate this achievement, ARRA Hotels’ Human Resources office, based in ARRA’s main Italian establishment, has organized a team event for its 420 employees and their families at its hotel in Spain.

Upon arrival at the hotel, each employee and family member is given an electronic wristband at the reception desk. The wristband serves a number of functions:

. Allows access to the “party zone” of the hotel, and emits a buzz if the user approaches any unauthorized areas

. Allows up to three free drinks for each person of legal age, and emits a buzz once this limit has been reached

. Grants a unique ID number for participating in the games and contests that have been planned.

Along with the wristband, each guest receives a QR code that leads to the online privacy notice describing the use of the wristband. The page also contains an unchecked consent checkbox. In the case of employee family members under the age of 16, consent must be given by a parent.

Among the various activities planned for the event, ARRA Hotels’ HR office has autonomously set up a photocall area, separate from the main event venue, where employees can come and have their pictures taken in traditional carnival costume.

The photos will be posted on ARRA Hotels’ main website for general marketing purposes.

On the night of the event, an employee from one of ARRA’s Greek hotels is displeased with the results of the photos in which he appears. He intends to file a complaint with the relevant supervisory authority in regard to the following:

. The lack of any privacy notice in the separate photocall area

The unlawful cross-border processing of his personal data

. The unacceptable aesthetic outcome of his photos

Assuming that there is a cross-border processing of personal data, which of the following criteria would NOT be useful to the lead supervisory authority responsible for the Greek employee’s complaint when trying to determine the location of the controller’s main establishment?

* Where the controller is registered as a company.
* Where the processor is registered as a company.
* Where decisions about the processing activities are made.
* Where the director with responsibility for processing activities is located.

Step by Step Guide to Prepare for CIPP-E Exam: https://www.vceprep.com/CIPP-E-latest-vce-prep.html]