Pass Your Next CIPP-E Certification Exam Easily & Hassle Free [Q134-Q157

Pass Your Next CIPP-E Certification Exam Easily & Hassle Free Free IAPP CIPP-E Exam Question Practice Exams

IAPP CIPP-E (Certified Information Privacy Professional/Europe (CIPP/E)) Certification Exam is a globally recognized certification that is sought after by professionals in the field of data privacy. It is designed to assess the knowledge and skills required to implement and manage a comprehensive data protection program within an organization that is compliant with European data protection laws and regulations. Certified Information Privacy Professional/Europe (CIPP/E) certification is awarded by the International Association of Privacy Professionals (IAPP) and is recognized by data protection authorities worldwide.

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.

Q134. What term BEST describes the European model for data protection?

* Sectoral
* Self-regulatory
* Market-based
* Comprehensive

Q135. 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.

Q136. 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.

Reference https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact- assessments

Q137. SCENARIO

Please use the following to answer the next question:

Ben is a member of the fitness club STAYFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Ben lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Ben was photographed while working out at a branch of STAYFIT in Frankfurt, Germany. At the time, Ben gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club’s U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Ben no longer feels comfortable with his photograph being publicly associated with the fitness club.

After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Ben sends a letter to STAYFIT requesting that his image be removed from the website and all promotional materials. Months pass and Ben, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact STAYFIT through alternate channels, he decides to take action against the company.

Ben contacts the U.K. Information Commissioner’s Office (‘ICO’ – the U.K.’s supervisory authority) to lodge a complaint about this matter.

Under the cooperation mechanism, what should the lead authority (the CNIL) do after it has formed its view on the matter?
* Submit a draft decision to other supervisory authorities for their opinion.
* Request that the other supervisory authorities provide the lead authority with a draft decision for its consideration.
* Submit a draft decision directly to the Commission to ensure the effectiveness of the consistency mechanism.
* Request that members of the seconding supervisory authority and the host supervisory authority co-draft a decision.

Q138. 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 would MOST effectively assist Zandelay in conducting their data protection impact assessment?
* Information about DPIAs found in Articles 38 through 40 of the GDPR.
* Data breach documentation that data controllers are required to maintain.
* Existing DPIA guides published by local supervisory authorities.
* Records of processing activities that data controllers are required to maintain.

Q139. SCENARIO

Please use the following to answer the next question:

Sandy recently joined Market4U, an advertising technology company founded in 2016, as their VP of Privacy and Data Governance. Through her first initiative in conducting a data inventory, Sandy learned that Market4U maintains a list of 19 million global contacts that were collected throughout the course of Market4U’s existence. Knowing the risk of having such a large amount of data, Sandy wanted to purge all contacts that were entered into Market4U’s systems prior to May 2018, unless such contacts had a more recent interaction with Market4U content. However, Dan, the VP of Sales, informed Sandy that all of the contacts provide useful information regarding successful marketing campaigns and trends in industry verticals for Market4U’s clients.

Dan also informed Sandy that he had wanted to focus on gaining more customers within the sports and entertainment industry. To assist with this behavior, Market4U’s marketing team decided to add several new fields to Market4U’s website forms, including forms for downloading white papers, creating accounts to participate in Market4U’s forum, and attending events. Such fields include birth date and salary.

What is the best way that Sandy can gain the insights that Dan seeks while still minimizing risks for Market4U?
* Conduct analysis only on anonymized personal data.
* Conduct analysis only on pseudonymized personal data.
* Delete all data collected prior to May 2018 after conducting the trend analysis.
* Procure a third party to conduct the analysis and delete the data from Market4U’s systems.

Q140. If a data subject puts a complaint before a DPA and receives no information about its progress or outcome, how long does the data subject have to wait before taking action in the courts?

* 1 month.
* 3 months.
* 5 months.
* 12 months.

Q141. 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 https://www.itgovernance.co.uk/blog/gdpr-lawful-bases-for-processing-with-examples

Q142. Which statement provides an accurate description of a directive?
* 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
* A directive has binding legal force throughout every member state and enters into force on a set date in all the member states.
* A directive is a legal act relating to specific cases and directed towards member states, companies 0′ private individuals.
* A directive is a legal act that applies automatically and uniformly to all EU countries as soon as it enters into force.

Q143. Tanya is the Data Protection Officer for Curtains Inc., a GDPR data controller. She has recommended that the company encrypt all personal data at rest. Which GDPR principle is she following?
* Accuracy
* Storage Limitation
* Integrity and confidentiality
* Lawfulness, fairness and transparency

Explanation/Reference: https://www.icaew.com/technical/technology/data/data-protection/data-protection-articles/do-i-have-to-encrypt-personal-data-to-comply-with-dpa-2018

Q144. Which sentence BEST summarizes the concepts of “fairness,” “lawfulness” and “transparency”, as expressly required by Article 5 of the GDPR?
* Fairness and transparency refer to the communication of key information before collecting data; lawfulness refers to compliance with government regulations.
* Fairness refers to limiting the amount of data collected from individuals; lawfulness refers to the approval of company guidelines by the state; transparency solely relates to communication of key information before collecting data.
* Fairness refers to the security of personal data; lawfulness and transparency refers to the analysis of ordinances to ensure they are uniformly enforced.
* Fairness refers to the collection of data from diverse subjects; lawfulness refers to the need for legal rules to be uniform; transparency refers to giving individuals access to their data.

Q145. Which of the following is NOT recognized as being a common characteristic of cloud-computing services?
* The service’s infrastructure is shared among the supplier’s customers and can be located in a number of countries.
* The supplier determines the location, security measures, and service standards applicable to the processing.
* The supplier allows customer data to be transferred around the infrastructure according to capacity.
* The supplier assumes the vendor’s business risk associated with data processed by the supplier.

Reference https://www.softwaremajor.com/news-articles/64-gdpr-how-does-it-apply-to-the-cloud

Q146. 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.

Q147. Tanya is the Data Protection Officer for Curtains Inc., a GDPR data controller. She has recommended that the company encrypt all personal data at rest. Which GDPR principle is she following?
* Accuracy
* Storage Limitation
* Integrity and confidentiality
* Lawfulness, fairness and transparency
Reference https://www.icaew.com/technical/technology/data/data-protection/data-protection-articles/do-i-have-to-encrypt-personal-data-to-comply-with-dpa-2018

Q148. Company X has entrusted the processing of their payroll data to Provider Y.

Provider Y stores this encrypted data in its server. The IT department of Provider Y finds out that someone managed to hack into the system and take a copy of the data from its server. In this scenario, whom does Provider Y have the obligation to notify?
* The public
* Company X
* Law enforcement
* The supervisory authority

Q149. What is the most frequently used mechanism for legitimizing cross-border data transfer?
* Standard Contractual Clauses.
* Approved Code of Conduct.
* Binding Corporate Rules.
* Derogations.
Reference https://www.dataguidance.com/opinion/international-eu-us-cross-border-data-transfers

Q150. When hiring a data processor, which action would a data controller NOT be able to depend upon to avoid liability in the event of a security breach?
* Documenting due diligence steps taken in the pre-contractual stage.
* Conducting a risk assessment to analyze possible outsourcing threats.
* Requiring that the processor directly notify the appropriate supervisory authority.
* Maintaining evidence that the processor was the best possible market choice available.

Q151. A German data subject was the victim of an embarrassing prank 20 years ago. A newspaper website published an article about the prank at the time, and the article is still available on the newspaper’s website. Unfortunately, the prank is the top search result when a user searches on the victim’s name. The data subject requests that SearchCo delist this result. SearchCo agrees, and instructs its technology team to avoid scanning or indexing the article. What else must SearchCo do?
* Notify the newspaper that its article it is delisting the article.
* Fully erase the URL to the content, as opposed to delist which is mainly based on data subject’s name.
* Identify other controllers who are processing the same information and inform them of the delisting request.
* Prevent the article from being listed in search results no matter what search terms are entered into the search engine.

Q152. If a multi-national company wanted to conduct background checks on all current and potential employees, including those based in Europe, what key provision would the company have to follow?
* Background checks on employees could be performed only under prior notice to all employees.
* Background checks are only authorized with prior notice and express consent from all employees including those based in Europe.
* Background checks on European employees will stem from data protection and employment law, which can vary between member states.

* Background checks may not be allowed on European employees, but the company can create lists based on its legitimate interests, identifying individuals who are ineligible for employment.

Q153. What is the key difference between the European Council and the Council of the European Union?
* The Council of the European Union is helmed by a president.
* The Council of the European Union has a degree of legislative power.
* The European Council focuses primarily on issues involving human rights.
* The European Council is comprised of the heads of each EU member state.

Section: (none)

Explanation

Q154. 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 would MOST effectively assist Zandelay in conducting their data protection impact assessment?
* Information about DPIAs found in Articles 38 through 40 of the GDPR.
* Data breach documentation that data controllers are required to maintain.
* Existing DPIA guides published by local supervisory authorities.
* Records of processing activities that data controllers are required to maintain.

Q155. Which of the following is NOT an explicit right granted to data subjects under the GDPR?
* The right to request access to the personal data a controller holds about them.
* The right to request the deletion of data a controller holds about them.
* The right to opt-out of the sale of their personal data to third parties.
* The right to request restriction of processing of personal data, under certain scenarios.

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

Q156. 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.

Q157. 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”
* No, the assessors do not quality as data processors as they only have access to encrypted data.
* No. the assessors do not quality as data processors as they do not copy the data to their facilities.
* Yes. the assessors a-e considered to be joint data controllers and must sign a mutual data processing agreement.
* Yes, the assessors are data processors and their processing of personal data must be governed by a separate contract or other legal act.

Ace CIPP-E Certification with 252 Actual Questions: https://www.braindumpsit.com/CIPP-E_real-exam.html]