This page was exported from - Exams Labs Braindumps
Export date: Fri Jul 5 18:29:26 2024 / +0000 GMT

TAKE Certified Information Privacy Professional CIPP-E PRACTICE QUESTIONS FOR AMAZING RESULTS [Q88-Q106

TAKE Certified Information Privacy Professional CIPP-E PRACTICE QUESTIONS FOR AMAZING RESULTS
IAPP CIPP-E Exam Dumps Are Essential To Get Good Marks

QUESTION 88

The GDPR requires controllers to supply data subjects with detailed information about the processing of their dat a. Where a controller obtains data directly from data subjects, which of the following items of information does NOT legally have to be supplied?

* The recipients or categories of recipients.
* The categories of personal data concerned.
* The rights of access, erasure, restriction, and portability.
* The right to lodge a complaint with a supervisory authority.

Reference https://gdpr-info.eu/art-13-gdpr/

QUESTION 89

SCENARIO

Please use the following to answer the next question:

Jason, a long-time customer of ABC insurance, was involved in a minor car accident a few months ago.

Although no one was hurt, Jason has been plagued by texts and calls from a company called Erbium Insurance offering to help him recover compensation for personal injury. Jason has heard about insurance companies selling customers’ data to third parties, and he’s convinced that Erbium must have gotten his information from ABC.

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

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

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

ABC supplies Jason with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Jason it cannot transfer his data directly to Xentron at this is not technically feasible. ABC also explains that Jason’s contract included a provision whereby Jason agreed that his data could be used for marketing purposes; according to ABC, it is too late for Jason to change his mind about this. It angers Jason when he recalls the wording of the contract, which was filled with legal jargon and very confusing.

In the meantime, Jason is still receiving unwanted calls from Erbium Insurance. He writes to Erbium to ask for the name of the organization that supplied his details to them. He warns Erbium 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.

Erbium’s response letter confirms Jason’s suspicions. Erbium is ABC’s wholly owned subsidiary, and they received information about Jason’s accident from ABC shortly after Jason submitted his accident claim.

Erbium assures Jason that there has been no breach of the GDPR, as Jason’s contract included a provision in which he agreed to share his information with ABC’s affiliates for business purposes.

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

Which statement accurately summarizes ABC’s obligation in regard to Jason’s data portability request?
* ABC does not have a duty to transfer Jason’s data to Xentron if doing so is legitimately not technically feasible.
* ABC does not have to transfer Jason’s data to Xentron because the right to data portability does not apply where personal data are processed in order to carry out tasks in the public interest.
* ABC has failed to comply with the duty to transfer Jason’s data to Xentron because the duty applies wherever personal data are processed by automated means and necessary for the performance of a contract with the customer.
* ABC has failed to comply with the duty to transfer Jason’s data to Xentron 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.

QUESTION 90

A data controller appoints a data protection officer. Which of the following conditions would NOT result in an infringement of Articles 37 to 39 of the GDPR?
* If the data protection officer lacks ISO 27001 auditor certification.
* If the data protection officer is provided by the data processor.
* If the data protection officer also manages the marketing budget.
* If the data protection officer receives instructions from the data controller.
Reference https://www.itgovernance.eu/fr-lu/data-protection-officer-dpo-under-the-gdpr-lu

QUESTION 91

Which of the following is one of the supervisory authority’s investigative powers?
* To notify the controller or the processor of an alleged infringement of the GDPR.
* To require that controllers or processors adopt approved data protection certification mechanisms.
* To determine whether a controller or processor has the right to a judicial remedy concerning a compensation decision made against them.
* To require data controllers to provide them with written notification of all new processing activities.
Reference https://gdpr-info.eu/art-58-gdpr/

QUESTION 92

SCENARIO

Please use the following to answer the next question:

WonderkKids provides an online booking service for childcare. Wonderkids is based in France, but hosts its website through a company in Switzerland. As part of their service, WonderKids will pass all personal data provided to them to the childcare provider booked through their system. The type of personal data collected on the website includes the name of the person booking the childcare, address and contact details, as well as information about the children to be cared for including name, age, gender and health information. The privacy statement on Wonderkids’ website states the following:

“WonderkKids provides the information you disclose to us through this website to your childcare provider for scheduling and health and safety reasons. We may also use your and your child’s personal information for our own legitimate business purposes and we employ a third-party website hosting company located in Switzerland to store the dat a. Any data stored on equipment located in Switzerland meets the European Commission provisions for guaranteeing adequate safeguards for you and your child’s personal information. We will only share you and your child’s personal information with businesses that we see as adding real value to you. By providing us with any personal data, you consent to its transfer to affiliated businesses and to send you promotional offers.”

“We may retain you and your child’s personal information for no more than 28 days, at which point the data will be depersonalized, unless your personal information is being used for a legitimate business purpose beyond 28 days where it may be retained for up to 2 years.”

“We are processing you and your child’s personal information with your consent. If you choose not to provide certain information to us, you may not be able to use our services. You have the right to: request access to you and your child’s personal information; rectify or erase you or your child’s personal information; the right to correction or erasure of you and/or your child’s personal information; object to any processing of you and your child’s personal information. You also have the right to complain to the supervisory authority about our data processing activities.” What must the contract between WonderKids and the hosting service provider contain?
* The requirement to implement technical and organizational measures to protect the data.

* Controller-to-controller model contract clauses.
* Audit rights for the data subjects.
* A non-disclosure agreement.

QUESTION 93

Bioface is a company based in the United States. It has no servers, personnel or assets in the European Union. By collecting photographs from social media and other web-based services, such as newspapers and blogs, it uses machine learning to develop a facial recognition algorithm. The algorithm identifies individuals in photographs who are not in its data set based the algorithm and its existing dat a. The service collects photographs of data subjects in the European Union and will identify them if presented with their photographs. Bioface offers its service to government agencies and companies in the United States and Canada, but not to those in the European Union. Bioface does not offer the service to individuals.

Why is Bioface subject to the territorial scope of the General Data Protection Regulation?
* It collects data from European Union websites, which constitutes an establishment in the European Union.
* It offers services in the European Union by identifying data subjects in the European Union.
* It collects data from subjects and uses it for automated processing.
* It monitors the behavior of data subjects in the European Union.

QUESTION 94

In 2016’s Guidance, the United Kingdom’s Information Commissioner’s Office (ICO) reaffirmed the importance of using a “layered notice” to provide data subjects with what?
* A privacy notice containing brief information whilst offering access to further detail.
* A privacy notice explaining the consequences for opting out of the use of cookies on a website.
* An explanation of the security measures used when personal data is transferred to a third party.
* An efficient means of providing written consent in member states where they are required to do so.

Explanation

QUESTION 95

Which mechanism, new to the GDPR, now allows for the possibility of personal data transfers to third countries under Article 42?
* Approved certifications.
* Binding corporate rules.
* Law enforcement requests.
* Standard contractual clauses.

Reference https://www.anonos.com/gdpr-chapter-5-transfers-of-personal-data-to-third-countries-or- international-organisations

QUESTION 96

SCENARIO

Please use the following to answer the next question:

Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees’ computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other

features, including the monitoring of employees’ computers.

Since these measures would potentially impact employees, Building Block’s Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.

After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees’ computers activity and their location.

During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization. The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased.

Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company’s computers, and from working remotely without authorization.

What would be the MOST APPROPRIATE way for Building Block to handle the situation with the employee from Italy?
* Since the GDPR does not apply to this situation, the company would be entitled to apply any disciplinary measure authorized under Italian labor law.
* Since the employee was the cause of a serious risk for the server performance and their data, the company would be entitled to apply disciplinary measures to this employee, including fair dismissal.
* Since the employee was not informed that the security measures would be used for other purposes such as monitoring, the company could face difficulties in applying any disciplinary measures to this employee.
* Since this was a serious infringement, but the employee was not appropriately informed about the consequences the new security measures, the company would be entitled to apply some disciplinary measures, but not dismissal.

QUESTION 97

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
Reference https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/ adequacy-decisions_en

QUESTION 98

Which of the following was the first to implement national law for data protection in 1973?
* France
* Sweden
* Germany
* United Kingdom
Reference https://scandinavianlaw.se/pdf/47-18.pdf

QUESTION 99

A grade school is planning to use facial recognition to track student attendance. Which of the following may provide a lawful basis for this processing?

* The school places a notice near each camera.
* The school gets explicit consent from the students.
* Processing is necessary for the legitimate interests pursed by the school.
* A state law requires facial recognition to verify attendance.

Reference https://www.jdsupra.com/legalnews/let-s-face-it-facial-recognition-1134180/

QUESTION 100

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 101

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.

Explanation

QUESTION 102

What was the aim of the European Data Protection Directive 95/46/EC?

* To harmonize the implementation of the European Convention of Human Rights across all member states.
* To implement the OECD Guidelines on the Protection of Privacy and trans-border flows of Personal Data.
* To completely prevent the transfer of personal data out of the European Union.
* To further reconcile the protection of the fundamental rights of individuals with the free flow of data from one member state to another.

Reference https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (3)

QUESTION 103

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.

QUESTION 104

According to the GDPR, how is pseudonymous personal data defined?
* Data that can no longer be attributed to a specific data subject without the use of additional information kept separately.
* Data that can no longer be attributed to a specific data subject, with no possibility of re-identifying the data.
* Data that has been rendered anonymous in such a manner that the data subject is no longer identifiable.
* Data that has been encrypted or is subject to other technical safeguards.

Explanation/Reference: https://www.chino.io/blog/what-is-pseudonymous-data-according-to-the-gdpr/

QUESTION 105

SCENARIO

Please use the following to answer the next question:

Anna and Frank both work at Granchester University. Anna is a lawyer responsible for data protection, while Frank is a lecturer in the engineering department. The University maintains a number of types of records:

Student records, including names, student numbers, home addresses, pre-university information, university attendance and performance records, details of special educational needs and financial information.

Staff records, including autobiographical materials (such as curricula, professional contact files, student evaluations and other relevant teaching files).

Alumni records, including birthplaces, years of birth, dates of matriculation and conferrals of degrees. These records are available to former students after registering through Granchester’s Alumni portal. Department for Education records, showing how certain demographic groups (such as first-generation students) could be expected, on average, to progress. These records do not contain names or identification numbers.

Under their security policy, the University encrypts all of its personal data records in transit and at rest.

In order to improve his teaching, Frank wants to investigate how his engineering students perform in relational to Department for Education expectations. He has attended one of Anna’s data protection training courses and knows that he should use no more personal data than necessary to accomplish his goal. He creates a program that will only export some student data: previous schools attended, grades originally obtained, grades currently obtained and first time university attended. He wants to keep the records at the individual student level. Mindful of Anna’s training, Frank runs the student numbers through an algorithm to transform them into different reference numbers. He uses the same algorithm on each occasion so that he can update each record over time.

One of Anna’s tasks is to complete the record of processing activities, as required by the GDPR. After receiving her email reminder, as required by the GDPR. After receiving her email reminder, Frank informs Anna about his performance database.

Ann explains to Frank that, as well as minimizing personal data, the University has to check that this new use of existing data is permissible. She also suspects that, under the GDPR, a risk analysis may have to be carried out before the data processing can take place. Anna arranges to discuss this further with Frank after she has done some additional research.

Frank wants to be able to work on his analysis in his spare time, so he transfers it to his home laptop (which is not encrypted). Unfortunately, when Frank takes the laptop into the University he loses it on the train. Frank has to see Anna that day to discuss compatible processing. He knows that he needs to report security incidents, so he decides to tell Anna about his lost laptop at the same time.

Anna will find that a risk analysis is NOT necessary in this situation as long as?

* The data subjects are no longer current students of Frank’s
* The processing will not negatively affect the rights of the data subjects
* The algorithms that Frank uses for the processing are technologically sound
* The data subjects gave their unambiguous consent for the original processing

QUESTION 106

Under what circumstances might the “soft opt-in” rule apply in relation to direct marketing?
* When an individual has not consented to the marketing.
* When an individual’s details are obtained from their inquiries about buying a product.
* Where an individual’s details have been obtained from a bought-in marketing list.
* Where an individual is given the ability to unsubscribe from marketing emails sent to him.

Latest IAPP CIPP-E Dumps with Test Engine and PDF (New Questions):
https://www.examslabs.com/IAPP/Certified-Information-Privacy-Professional/best-CIPP-E-exam-dumps.html]