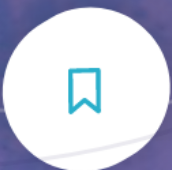


CIPP/E EXAM QUESTIONS



CIPPTraining.com

**SAMPLE PRACTICE
QUESTIONS
CIPP/E**



CIPP/E Practice Exam Questions

Practice questions are indispensable for good exam preparation. Below you will find thirty IAPP style CIPP/E practice exam questions including two scenario questions.

The sample questions are part of our CIPP/E online training course. Our courses contain more than 300 of these practice questions. More information can be found at CIPPTraining.com.

1. The first rules to balance personal freedom with restrictions of rights are found in...

- A. The Charter of Fundamental Rights and the Treaty of Lisbon
- B. The European data protection package
- C. The Universal Declaration of Human Rights of the United Nations and the European Convention on Human Rights (ECHR)
- D. The OECD guidelines

2. (What is the BEST answer?) A controller...

- A. Follows the instructions of the processor
- B. Processes the data and ensures the regulations are followed
- C. Determines the status of parties that process personal data
- D. Determines for what purposes personal data is processed

3. In Convention 109 and Article 5 of the GDPR, it's set that in order to process data legally, it must be _____, which means that the subjects must be aware that their personal data is used.

- A. lawful
- B. fair
- C. with consent
- D. transparent

4. Data subjects have the right to freeze their data if they requested erasure. This falls under...

- A. Article 15 - right of access
- B. Article 16 - right to rectification
- C. Article 17 - right to erasure
- D. Article 18 - right to restriction of processing

5. The three mechanisms under which personal data can be transferred outside the European Economic Area (EEA) are...

- A. public authority, appropriate safeguards, and specific situations
- B. public authority, adequate findings, and special categories
- C. scope, adequate findings, and appropriate safeguards
- D. adequate findings, appropriate safeguards, and under specific derogations

6. Is location data a form of personal data?

- A. No, because a person can't be identified using it
- B. No, because it's not private information
- C. Yes, because a person can be identified using it
- D. Yes, because it's private information

7. The ePrivacy Regulation was changed in 2009. What was the biggest change?

- A. The inclusion of all electronic devices
- B. Ensuring consistency with the GDPR
- C. Users have to consent to cookies
- D. Simplification of the rules..

8. A surveying agency has the name of a person and their political opinions. What kind of data is the latter?

- A. Anonymous information
- B. Non-personal data
- C. Personal data
- D. Sensitive data

9. Which of the following is NOT the scope of the GDPR?

- A. Organizations not based in Europe
- B. Not-for-profit organizations
- C. Households
- D. Healthcare institutions

Use the following scenario to answer questions 10-14.

One Case, One Phone (OCOP) is a company that sells customizable cases for cellphones. They are based in Germany and have two physical shops, one in Berlin and one in Stuttgart. However, most of their profits come from their online shop. The website uses cookies for better performance and they collect data from customers worldwide.

They have grown and can't keep up with the orders in their small workshop in Germany. Because of this, OCOP has contacted a Japanese factory that would be able to build the cases and then send them to the customers. To do that, they need to know the customer's name as well as their phone model. They wouldn't require any other data, such as credit card numbers, nationalities, or age. This data would only be stored in the German database.

OCOP has investigated the Japanese factory and has found they have never had a data breach, although they don't follow all the principles of the GDPR.

In November 2020, the Japanese factory had to deal with a major data breach. The data of at least 500 Germans and Swiss were lost. Furthermore, data of Brazilians has also been lost.

10. Is OCOP allowed to transfer the customer's name and the phone model to a factory in another country? What is the BEST answer?

- A. Yes, since it follows the principle of necessity
- B. Yes, in principle, but a distinction must be made between countries
- C. No, data can never be transferred internationally
- D. No, data can only be transferred internationally for medical or security reasons

11. Is OCOP allowed to transfer the data to the Japanese factory?

- A. Yes, because they offer an adequate level of protection
- B. No, because they don't offer an adequate level of protection
- C. Yes, because it follows the principle of necessity
- D. No, because it doesn't follow the principle of necessity

12. Regarding the cookies, is it allowed (privacy compliant) to use them?

- A. Yes, they can use them as long as they are necessary for efficiency
- B. Yes, but only if they give detailed information about them to the customers
- C. Yes, but only if they give detailed information about them to the customers, as well as their consent
- D. Yes, but only if they give detailed information about them to the customers, as well as their consent, and there is an option to visit the website without using them

13. The Japanese factory tells OCOP they want to have the customer's age as well. They argue this will allow for a more targeted design, as well as less confusion with orders. Can OCOP send them this information? What is the BEST answer?

- A. Yes, since it follows or principles on the GDPR
- B. Yes, they can transfer any data as long as it's safe
- C. No, because it doesn't follow the principle of necessity
- D. No, because it doesn't follow the principle of adequacy

14. OCOP wants to review online privacy rights to make sure they are following them appropriately. What should they consult?

- A. Convention 108
- B. Data Protection Directive
- C. Data Retention Directive
- D. The ePrivacy Directive

15. The principles for data processing are stated in...

- A. Article 5 of the GDPR
- B. Article 6 of the GDPR
- C. Article 5 of Convention 109
- D. Article 6 of Convention 109+

16. A company asks users for their addresses in order to send a package they have ordered. Does this follow the principle of “necessity”?

- A. Yes, it’s considered a contract performance
- B. Yes, it’s considered a legitimate interest
- C. Yes, it’s considered a vital interest
- D. Yes, it’s considered a legal obligation

17. As of today, which of the following rights has an unclear scope?

- A. The right of access
- B. The right to not be subjected to profiling
- C. The right to data portability
- D. The right of transparent communication and information

18. The controller’s relationships with processors and sub-processors is part of...

- A. Liabilities
- B. Representative actions
- C. Self-regulation
- D. Code of Conduct

19. When a company processes an employee data to pay their salary, they will do the process on the basis of...

- A. Consent
- B. Employee’s legitimate interest
- C. Fulfilling the employee’s contract
- D. Legal obligation of the employee

20. Identifying the handwriting of an individual can be considered as...

- A. Communications data
- B. Video surveillance
- C. Biometric data
- D. Personal data

21. Can there be personal data in the Internet of Things?

- A. Yes, and it will all be public.
- B. Yes, and some will not be public
- C. No, because since it's public it's not personal data anymore
- D. No, it's about things not persons and personal data

22. Which of the following are recognized routes for data transfer outside the EEA?

- A. BCRs
- B. Alternative contractual mechanisms
- C. Standard contractual clauses
- D. All the above

23. What is considered sensitive data?

- A. Any personal data
- B. Any data that risks the rights or freedom of an individual
- C. Data that involves a large amount of people
- D. Data that is stored without the data subject's specific consent

24. Are EU agencies covered by the GDPR?

- A. Yes, always
- B. Only in the case of sensitive data
- C. Only if it involves more than one Member State
- D. No, never

25. Do companies have to report data processing to the DPA?

- A. Yes, all of them
- B. Only if they deal with sensitive data
- C. No, but they must keep records of data processing
- D. No, but they must keep records of sensitive data

Use the following scenario to answer questions 26-30.

Door to Door is a delivery agency. They have close partnerships with several European small manufacturing businesses and deliver delicate crafts to customers.

When one of the manufacturing businesses receives an order, they transfer the data of the type of product and the client's name, address, and phone number to Door to Door. The agency then passes that information on to one of their employees, who will start the delivery. The employee calls the customers to arrange a smooth delivery.

The customers are not informed about the involvement of Door to Door, and as far as they know, the personal information they provide only goes to the small business they made the purchase from. However, each of the businesses does inform the clients that their data is used for the delivery.

26. Delivery information is automatically shared with Door to Door. Should the manufacturing business inform clients that this kind of information will be shared?

- A. No, it's enough if they communicate who the controllers are
- B. No, but they should outline for which purposes the data is shared
- C. Yes, it's mandatory to provide the categories of recipients
- D. That depends on how they share data

27. Should Door to Door inform clients about the personal information it received? What is the BEST answer?

- A. Yes, because it's necessary to carry out their purchase and delivery
- B. Yes, and it would be under any circumstance
- C. Yes, the information obligation also applies if the information does not come directly from the customer
- D. No, Door to Door is not the controller

28. After ordering, a client requests not to have his telephone number shared with anyone. What would be the most appropriate response?

- A. This request comes too late
- B. The business should offer to delete all the data
- C. The business is not under an obligation to do anything
- D. The business should try to honor the request as much as possible

29. Door to Door wants to use the data from the clients to offer a personalized app with the business they buy more frequently from. Should the clients be informed?

- A. No, because it benefits the client
- B. No, because they have already agreed to share their data for this purpose
- C. Yes, they should receive the information
- D. Yes, they should give specific (informed) consent

30. One of the businesses provides comprehensive information about data subject's rights. They use precise language from the specific field of law. Is it mandatory to do this?

- A. Yes, the information should always be in legal terminology so it can be specific
- B. No, they should use common language
- C. The use of legal language is adequate, but the information provided should not be too comprehensive
- D. It's not mandatory, but it's not wrong either

References

1. Answer: C. A first point of departure was the Universal Declaration of Human Rights of the United Nations in 1948. A second point of reference is the European Convention on Human Rights (ECHR) from 1953. Both treaties recognize the balance between freedoms and rights of persons and the justified restriction of these rights.
2. Answer: D. A controller is the natural or legal person, the government agency, the office of another authority that alone or together with others determines the purpose and the means for the processing of the data.
3. Answer: B. The fundamental principles from Convention 109 and the directive are reflected in Articles 5 and 6 of the GDPR. It states the processing must be fair. This means that the data subject must be aware that his or her data is processed and used. Only in that case can a well-considered judgment be given.
4. Answer: D. Article 18: Right to restriction of processing. This right concerns temporary freezing of data. Data subjects have the right to restrict the processing of their personal data when verifying overriding grounds is pending in the context of an erasure request.
5. Answer: D. Transfer of personal data outside the European Economic Area (EEA) can legally take place in three ways (Articles 44-50), namely on the basis of: 1. 'Adequacy findings'- Article 45; 2. 'Appropriate safeguards'- Article 46; 3. 'Derogation for specific situations'- Article 49.
6. Answer: C. Location-based services (LBS) utilize information about location to deliver a wide array of applications and services (entertainment, navigation, payment). Location data are included in the definition of personal data. They can lead to the identification of a person.
7. Answer: C. The ePrivacy directive was amended in 2009. The most important change has to do with cookies. Article 5 paragraph 3 stipulates that the storage of information in the terminal equipment of a subscriber or user is only permitted on the condition that the user concerned has given his consent.
8. Answer: D. The regulation stipulates that some types of personal data require additional protection. The processing of these sensitive data can lead to a significant risk for individual fundamental rights and fundamental freedoms. This includes revealing racial or ethnic origin, political opinions, and religious or philosophical belief.
9. Answer: C. The material scope is laid down in Article 2. The scope is negatively defined by exceptions to households, the LEDP, and foreign and security policy of the EU and the EU institutions.
10. Answer B. One of the GDPR's objectives is to let information flow freely between states that commit to the principles of data protection. The GDPR contains various core concepts. "Necessity" is one of the core concepts. For the data processing and transfer to be lawful, the processing must be necessary. Special attention should be paid to the transfer of personal data to third countries.
11. Answer A. Adequacy is another concept. For example, the directive prohibits international data transfers to jurisdictions that do not offer an adequate level of protection. Japan ensures an 'adequate level of protection' as determined by the Commission (Article 45).

12. Answer C. In the ePrivacy Directive, Article 5 paragraph 3 stipulates that the storage of information in the terminal equipment of a subscriber or user is only permitted on condition that the user concerned has given his consent. For this, it must first be provided with clear and complete information.
13. Answer C. The GDPR contains various core concepts. "Necessity" is one of the core concepts. For the data processing to be lawful, the processing must be necessary. Producing and sending the case wouldn't require customer age. To avoid confusion, order numbers could also be used instead of age.
14. Answer D. They should include the ePrivacy Directive regarding cookies and the GDPR. Convention 108 and the Data Protection Directive are outdated. The Data Retention Directive is ruled invalid.
15. Answer A. The fundamental principles from Convention 109 and the former directive are reflected in Articles 5 and 6 of the GDPR. It sets out the principles for processing (Article 5) and the legal grounds for processing (Article 6).
16. Answer A. Contract performance: processing is necessary for the performance of a contract. For example, personal data is required for delivery of a product or service. Processing must be unavoidable in order to complete the contract.
17. Answer B. Article 22: Right to not be subjected to automated decision making (to profiling). The scope and application of this right is not yet entirely clear. In the coming years it will become clear what exactly this right entails.
18. Answer C. Accountability, as described in Chapter 11. A few components in the context of self-regulation include: the focus on demonstrable proof of compliance, controllers' relationships with processors and sub-processors, notification of personal data breaches to the DPAs and subjects, and the execution of DPIAs.
19. Answer C. Processing is necessary to fulfill the employment contract; for example, to pay the employee, the employer must process the employee's name and bank details.
20. Answer D. This is not so much about physical properties (biometric data), but the handwriting can uniquely identify a person.
21. Answer B. Many devices connected to the internet of things (IoT) have sensors with which they can collect information about their environment. This may be personal data. The requirement for personal data sent via these IoT networks is a challenge.
22. Answer D. The transfer of personal data outside the EEA is only allowed under certain conditions. The most common routes are BCRs, standard contractual clauses, and alternative contractual mechanisms.
23. Answer B. Sensitive data sharing is considered the revealing of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
24. Answer D. The EU institutions, bodies and agencies are not covered by the GDPR (which falls under Regulation 45/2001/C).

25. Answer C. Under the directive, companies had to report their processing to the DPA. This operation was cumbersome and has therefore been abolished. Instead of a notification, records must be kept of all processing operations. This register with records must be made available to a DPA upon request.

26. Answer C. Article 13(1) states the information obligations to data subjects. It requires the provision of a mandatory set of information. That information includes the identity of the controller, the contact details of the DPO, the purposes and legal basis of processing and the categories of recipients.

27. Answer D. Door to Door is not a controller and the client does not have to inform itself. In addition, the data is necessary to execute the agreement. That obligation rests on the manufacturing businesses (Article 13 and 14).

28. Answer D. Data subjects have several rights like the right to be forgotten, the right to restrict the processing of their data and the right to object. The manufacturing business can best find out why this request has been made and act accordingly.

29. Answer D. The intended use of the data is a use different than what was originally intended. Moreover, the clients did not provide their data to Door to Door but to the manufacturing businesses.

30. Answer B. If information is provided, in whatever form, controllers must ensure that it is clear, concise, and easy to understand in simple, unambiguous, and direct language. Information should be provided in a language that the data subjects are most likely to understand.

