IAPP CIPP-E Practice Questions

Shared by Stuart on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization receives a request multiple times from a data subject seeking to exercise his rights with respect to his own personal dat

a. Under what condition can the organization charge the data subject a fee for processing the request?

Options:

A- Only where the organization can show that it is reasonable to do so because more than one request was made.
B- Only to the extent this is allowed under the restrictions on data subjects' rights introduced under Art 23 of GDPR.
C- Only where the administrative costs of taking the action requested exceeds a certain threshold.
D- Only if the organization can demonstrate that the request is clearly excessive or misguided.

Answer:

D

Explanation:

According to the GDPR, data subjects have the right to access, rectify, erase, restrict, port and object to the processing of their personal data. These rights are not absolute and may be subject to limitations and conditions. One of these conditions is that the controller may charge a reasonable fee for the administrative costs of complying with the request if it is manifestly unfounded or excessive, in particular because of its repetitive character (Art 12(5) of GDPR). The controller has the burden of proving the manifestly unfounded or excessive character of the request. The fee must not exceed the actual costs incurred by the controller and must not prevent the exercise of the data subject's rights.Reference:

GDPR, Art 12(5)

Free CIPP/E Study Guide, p. 13

European Data Protection Law & Practice, p. 121

Question 2

Question Type: MultipleChoice

A company is hesitating between Binding Corporate Rules and Standard Contractual Clauses as a global data transfer solution. Which of the following statements would help the company make an effective decision?

Options:

A- Binding Corporate Rules are especially recommended for small and medium companies.
B- The data exporter does not need to be located in the EU for the standard Contractual Clauses.
C- Binding Corporate Rules provide a global solution for all the entities of a company that are bound by the intra-group agreement.
D- The company will need the prior authorization of all EU data protection authorities for concluding Standard Contractual Clauses.

Answer:

C

Explanation:

According to the GDPR, transfers of personal data to third countries or international organisations are only allowed if the controller or processor complies with the conditions laid down in Chapter V of the GDPR1.One of these conditions is the existence of an adequacy decision by the European Commission, which means that the third country or international organisation ensures an adequate level of protection for the personal data2.However, if there is no adequacy decision, the controller or processor must provide appropriate safeguards for the data transfer, such as binding corporate rules (BCR) or standard contractual clauses (SCC)3.

Binding corporate rules (BCR) are internal rules adopted by a group of undertakings or enterprises engaged in a joint economic activity, which define its global policy with regard to the international transfers of personal data within the same corporate group or business partners located in third countries4. BCR must include all the general data protection principles and enforceable rights to ensure appropriate safeguards for the data transfers.They must be legally binding and enforced by every member concerned of the group5.BCR must be approved by the competent supervisory authority in accordance with the consistency mechanism provided by the GDPR6.

Standard contractual clauses (SCC) are sets of contractual terms and conditions that the controller or processor and the recipient of the data agree to apply to the data transfer.SCC are adopted by the European Commission or by a supervisory authority in accordance with the consistency mechanism and are available in the Official Journal of the European Union7.SCC must offer sufficient safeguards on data protection for the data to be transferred

internationally8.

In the given scenario, option C is the statement that would help the company make an effective decision between BCR and SCC, as it highlights the main advantage of BCR over SCC, which is the global and comprehensive solution that BCR provide for all the entities of a company that are bound by the intra-group agreement. BCR are especially suitable for large and complex organisations that have frequent and high-volume data transfers within the same corporate group or business partners located in third countries. BCR also offer more flexibility and legal certainty than SCC, as they are tailored to the specific needs and structure of the group and do not require individual contracts for each data transfer.

The other options (A, B, and D) are either incorrect or misleading statements that would not help the company make an effective decision between BCR and SCC. Option A is incorrect, as BCR are not recommended for small and medium companies, but rather for large and complex ones, as explained above. Option B is misleading, as it implies that the data exporter can be located outside the EU for the SCC, which is true, but not relevant for the comparison with BCR, as the data exporter can also be located outside the EU for the BCR, as long as it is subject to the GDPR by virtue of Article 3(2). Option D is also misleading, as it implies that the company will need the prior authorization of all EU data protection authorities for concluding SCC, which is false, as the company will only need the prior authorization of the competent supervisory authority in the Member State where the data exporter is established, unless the SCC are modified or supplemented by additional clauses or safeguards.Reference:

1: [Article 44 of the GDPR]

2: [Article 45 of the GDPR]

3: [Article 46 of the GDPR]

4: [Article 4 (20) of the GDPR]

5: [Article 47 of the GDPR]

6: [Article 63 of the GDPR]

7: [Article 93 of the GDPR]

8: [Article 46 (2) and (d) of the GDPR]

: [Binding Corporate Rules (BCR)]

: [Article 3 (2) of the GDPR]

: [Article 46 (3) (a) and (b) of the GDPR]

: [Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)]

: [Binding Corporate Rules (BCR) - European Commission]

: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679]

:

[https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en]

: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679]

:
[https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en]

Question 3

Question Type: MultipleChoice

A key component of the OECD Guidelines is the ''Individual Participation Principle''. What parts of the General Data Protection Regulation (GDPR) provide the closest equivalent to that principle?

Options:

A- The lawful processing criteria stipulated by Articles 6 to 9
B- The information requirements set out in Articles 13 and 14
C- The breach notification requirements specified in Articles 33 and 34
D- The rights granted to data subjects under Articles 12 to 22

Answer:

D

Explanation:

:The Individual Participation Principle is one of the Fair Information Practice Principles (FIPPs) that are not part of any legal framework, but are widely adopted by many data privacy regulations in force today1. The FIPPs are a set of guidelines for fair information practices that aim to protect the privacy and security of personal information.The Individual Participation Principle holds that individuals have a number of rights, including the right to have their personal data corrected or erased, the right to access and obtain confirmation of their personal data, the right to be informed about how their personal data is used and who it is shared with, and the right to object or withdraw consent for certain purposes2.

The General Data Protection Regulation (GDPR) is a legal framework that implements the European Union's (EU) Data Protection Directive and provides comprehensive protection for all individuals within the EU regarding their personal data. The GDPR grants individuals a number of rights, such as the right to access, rectify, erase, restrict, port, object, or not be subject to

automated decision-making based on their personal data. These rights are similar to those under the FIPPs and can be found in Articles 12 to 22 of the GDPR.

Therefore, the parts of the GDPR that provide the closest equivalent to the Individual Participation Principle are Articles 12 to 22.

OECD Privacy Principles

What are the 7 main principles of GDPR?

Fair Information Practice Principles (FIPPs)

Individual Participation - International Association of Privacy Professionals

What is the right to be forgotten? | Right to erasure | Cloudflare

General Data Protection Regulation - Wikipedia

Question 4

Question Type: MultipleChoice

ISO 31700 has set forth requirements relating to consumer products and services. In particular, this international standard focuses on the implementation of which of the following?

Options:

A- Privacy by design.
B- Comprehensive ethical Al software.
C- Privacy notices for companies providing services to consumers.
D- Automated systems for identifying EU data subjects' personal data.

Answer:

A

Explanation:

ISO 31700 is an international standard that provides high-level requirements and recommendations for organizations that use privacy by design (PbD) in the development, maintenance and operation of consumer goods and services. PbD is a concept that aims to integrate privacy into products, services and systems by default, following seven main principles: proactive not reactive, privacy as the default, privacy embedded into design, full

functionality, end-to-end security, visibility and transparency, and respect for user privacy. PbD is also a legal requirement under many prominent privacy regulations across the world, such as the GDPR. ISO 31700 is based on a consumer-centric approach, where the consumer's privacy rights and preferences are placed at the center of product development and operation.

Question 5

Question Type: MultipleChoice

What should a controller do after a data subject opts out of a direct marketing activity?

Options:

A- Without exception, securely delete all personal data relating to the data subject.
B- Without undue delay, provide information to the data subject on the action that will be taken.
C- Refrain from processing personal data relating to the data subject for the relevant type of communication.
D- Take reasonable steps to inform third-party recipients that the data subject's personal data should be deleted and no longer processed.

Answer:

C

Explanation:

According to Article 21 of the GDPR, the data subject has the right to object at any time to the processing of his or her personal data for direct marketing purposes, which includes profiling related to such marketing. When the data subject exercises this right, the controller must stop processing the personal data for that purpose, unless it can demonstrate compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defense of legal claims. The controller must also inform the data subject of this right before the first communication with him or her, and in a clear and separate manner from other information. The controller must also provide the data subject with a simple and effective way to opt out of receiving direct marketing communications, such as an unsubscribe link or a STOP text message. The controller must respect the data subject's choice and refrain from sending any further direct marketing messages of the relevant type (e.g., email, phone, post, etc.) to the data subject, unless he or she opts in again. The controller does not need to delete the personal data of the data subject who opts out, unless the data subject also requests the erasure of his or her data under Article 17 of the GDPR, or the data is no longer necessary for the purposes for which it was collected or processed. The controller may also retain some minimal information about the data subject (such as name and email address) to ensure that his or her opt-out request is honored and that he or she is not contacted again for

direct marketing purposes. The controller must also ensure that any third parties to whom it has disclosed the personal data of the data subject for direct marketing purposes are informed of the opt-out request and comply with it, unless this proves impossible or involves disproportionate effort.Reference:Direct marketing rules and exceptions under the GDPR,Direct marketing and privacy and electronic communications,Marketing and advertising: the law: Direct marketing,Direct Marketing - What you need to know about direct marketing

Question 6

Question Type: MultipleChoice

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

Options:

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

Answer:

D

Explanation:

Under GDPR and EU employment law, employee monitoring must comply with the principles of necessity, proportionality, legitimacy, and transparency.

Legal requirements for employee monitoring:

Necessity: Employers must demonstrate that monitoring is necessary for a legitimate purpose.

Proportionality: The monitoring must be the least intrusive method available.

Transparency: Employees must be fully informed about what is being monitored.

Why is D the correct answer?

GDPR requires that monitoring must be explicitly communicated and justified.

Employers can monitor work emails, browsing history, and video calls, but only if employees are clearly informed and the purpose is justified.

Why are other answers incorrect?

A (Monitoring all contractor activity) Contractors have data protection rights too; monitoring must still be necessary and proportionate.

B (Daily consent requirement) Employee consent is not valid under GDPR in most cases due to power imbalance.

C (Monitoring in non-secure environments only) The location does not determine the lawfulness of monitoring.

Conclusion: The correct answer is D, as only explicitly marked and justified monitoring is lawful under GDPR.

Question 7

Question Type: MultipleChoice

Which change was introduced by the 2009 amendments to the e-Privacy Directive 2002/58/EC?

Options:

A- A voluntary notification for personal data breaches applicable to all data controllers.
B- A voluntary notification for personal data breaches applicable to electronic communication providers.
C- A mandatory notification for personal data breaches applicable to all data controllers.
D- A mandatory notification for personal data breaches applicable to electronic communication providers.

Answer:

D

Explanation:

The e-Privacy Directive 2002/58/EC, also known as the Directive on privacy and electronic communications, is a specific directive that complements and particularises the GDPR for the electronic communications sector. It was amended in 2009 by the Directive 2009/136/EC, which introduced several changes to enhance the protection of personal data and privacy in the electronic communications sector. One of these changes was the introduction of a mandatory

notification for personal data breaches applicable to providers of publicly available electronic communications services, such as telecom providers and internet service providers. According to Article 4 of the amended e-Privacy Directive, these providers must notify the competent national authority of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community. The notification must be made without undue delay and, where feasible, not later than 24 hours after the provider has become aware of the breach. The notification must include information such as the nature and content of the personal data concerned, the circumstances and consequences of the breach, and the measures taken or proposed by the provider to address the breach. The provider must also notify the affected data subjects of the breach, unless the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures that render the data unintelligible to any person who is not authorised to access it. The notification to the data subjects must describe the nature of the breach and the contact points where more information can be obtained, and must recommend measures to mitigate the possible adverse effects of the breach. The purpose of this mandatory notification is to ensure that the authorities and the data subjects are informed of the risks and the remedies related to the breach, and to encourage the providers to improve their security measures and prevent further breaches.Reference:e-Privacy Directive,Changes to e-Privacy Directive Approved by European Parliament,Article 2 Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications),Personal data breaches

Question 8

Question Type: MultipleChoice

Which of the following is NOT an explicit right granted to data subjects under the GDPR?

Options:

A- The right to request access to the personal data a controller holds about them.
B- The right to request the deletion of data a controller holds about them.
C- The right to opt-out of the sale of their personal data to third parties.
D- The right to request restriction of processing of personal data, under certain scenarios.

Answer:

C

Explanation:

This is not an explicit right granted to data subjects under the GDPR, as the GDPR does not

specifically address the sale of personal data.However, the GDPR does require that data subjects give their consent to any processing of their personal data that is not based on another legal basis, such as a contract or a legal obligation1.Therefore, data subjects have the right to withdraw their consent at any time, and the controller must inform them of this right before obtaining their consent2.The other options are explicit rights granted to data subjects under the GDPR, as they are listed in Chapter 3 of the regulation3.Reference:

Free CIPP/E Study Guide, page 23, section 3.1

CIPP/E Certification, page 18, section 3.1

The Ultimate CIPP/E Study Guide for 2023, page 16, section 3.1

GDPR data subject rights - 8 fundamental & additional rights, paragraph 4

Rights of the data subject - General Data Protection Regulation (GDPR), Article 7

Rights of the data subject - General Data Protection Regulation (GDPR), Chapter 3

Question 9

Question Type: MultipleChoice

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

Options:

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

Answer:

B

Explanation:

The use of facial recognition technology to track student attendance involves the processing of biometric data, which is a special category of personal data under the GDPR.Such data can only be processed under certain conditions, one of which is the explicit consent of the data subject1. Therefore, the school may provide a lawful basis for this processing if it obtains the explicit

consent of the students (or their legal guardians, if the students are minors).The consent must be freely given, specific, informed and unambiguous, and the students must have the right to withdraw their consent at any time2. The other options do not provide a lawful basis for this processing, as they do not meet the requirements for processing special categories of data.Placing a notice near each camera does not constitute consent, nor does it comply with the transparency principle3.Processing for the legitimate interests of the school may be a valid basis for processing personal data in general, but not for processing biometric data, unless it is authorised by a specific law that provides suitable safeguards4.A state law that requires facial recognition to verify attendance may also be a valid basis for processing personal data in general, but not for processing biometric data, unless it is necessary for reasons of substantial public interest and provides suitable safeguards5.Reference:

Free CIPP/E Study Guide, page 24, section 3.2

CIPP/E Certification, page 19, section 3.2

Cipp-e Study guides, Class notes & Summaries, page 17, section 3.2

Special categories of personal data - General Data Protection Regulation (GDPR), Article 9

Consent - General Data Protection Regulation (GDPR), Article 7

Principles - General Data Protection Regulation (GDPR), Article 5

Lawfulness of processing - General Data Protection Regulation (GDPR), Article 6

Special categories of personal data - General Data Protection Regulation (GDPR), Article 9