Free Questions for CIPP-E by braindumpscollection

Shared by Ferrell on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SCENARIO

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 he required access.

The company conducted an initial search of its IT systems, which returned a large amount of information They then contacted Jack, requesting that he be more specific regarding what information he required, so that they could carry out a targeted search Jack responded by stating that he would not narrow the scope of the information requester.

What would be the most appropriate response to Jacks data subject access request?

Options:

A- The company should not provide any information, as the company is headquartered outside of the EU.

B- The company should decline to provide any information, as the amount of information requested is too excessive to provide in one month.

C- The company should cite the need for an extension, and agree to provide the information requested in Jack's original DSAR within a period of 3 months.

D- The company should provide all requested information except for the emails, as they are excluded from data access request requirements under the GDPR.

Answer:

B

Explanation:

According to Article 15 of the GDPR, data subjects have the right to access and receive a copy of their personal data, and other supplementary information, from the data controller1. However, this right is not absolute and may be subject to limitations or restrictions.One of the grounds for refusing or limiting a data subject access request (DSAR) is when the request is manifestly unfounded or excessive, in particular because of its repetitive character1.In such cases, the controller may either charge a reasonable

fee, taking into account the administrative costs of providing the information, or refuse to act on the request1.The controller must inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy1.

In this scenario, Jack's DSAR is likely to be considered excessive, as he requests a copy of all personal data, including internal emails, that were sent or received by him or where he is directly or indirectly identifiable from the contents. This is a very broad and vague request, which would require the company to search and review a large amount of information, and potentially disclose confidential or sensitive data about other employees or third parties. The company has already contacted Jack, asking him to be more specific about what information he requires, but he refused to narrow the scope of his request.Therefore, the company has a valid reason to decline to provide any information, as the amount of information requested is too excessive to provide in one month, which is the general time limit for responding to a DSAR under the GDPR1. Therefore, option B is the correct answer.

Option A is incorrect because the company's headquarters location is irrelevant for the purpose of the DSAR, as the GDPR applies to any processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not2. The company has an establishment in Ireland, where Jack worked, and therefore is subject to the GDPR.

Option C is incorrect because the company cannot agree to provide the information requested in Jack's original DSAR within a period of 3 months, as this would violate the data subject's right of access and the principle of accountability under the GDPR.The company can only extend the time limit to respond to a DSAR by a further two months if the request is complex or if the controller receives a number of requests from the same data subject1.However, the company must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay1. In this case, the company has not done so, and has instead asked Jack to be more specific about his request.

Option D is incorrect because the company cannot provide all requested information except for the emails, as this would not comply with the data subject's right of access and the principle of transparency under the GDPR.The company must provide the data subject with a

copy of the personal data undergoing processing, unless this adversely affects the rights and freedoms of others1. The emails are part of the personal data undergoing processing, and the company cannot exclude them from the DSAR without a valid reason.The company must also provide the data subject with the following supplementary information, unless the data subject already has it1:

the purposes of the processing;

the categories of personal data concerned;

the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

the right to lodge a complaint with a supervisory authority;

where the personal data are not collected from the data subject, any available information as to their source;

the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Right of access

Territorial scope

Question 2

Question Type: MultipleChoice

SCENARIO

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 he required access.

The company conducted an initial search of its IT systems, which returned a large amount of information They then contacted Jack, requesting that he be more specific regarding what information he required, so that they could carry out a targeted search Jack responded by stating that he would not narrow the scope of the information requester.

Under Article 82 of the GDPR ("Right to compensation and liability-), which party is liable for the damage caused by the data breach?

Options:

A- Both parties are exempt, as the company is involved in human health research

B- Jack and the pharmaceutical company are jointly liable.

C- The pharmaceutical company is liable.

D- Jack is liable

Answer:

D

Explanation:

Article 82 of the GDPR introduces a right to compensation for damage caused as a result of an infringement of the GDPR1.Article 82 (1) states that any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered1.Article 82 (2) states that any controller involved in processing shall be liable for the damage caused by processing which infringes the GDPR1.A processor shall be liable for the damage

caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller1.Article 82 (3) states that a controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage1. In this case, Jack is liable for the damage caused by the data breach, as he violated the GDPR by posting the patient's name and health information, along with disparaging comments, on a social media website.This constitutes an infringement of the GDPR, as it violates the principles of lawfulness, fairness, and transparency (Article 5 (1) (a)), purpose limitation (Article 5 (1) (b)), data minimisation (Article 5 (1)), accuracy (Article 5 (1) (d)), integrity and confidentiality (Article 5 (1) (f)), and the rights of the data subject (Articles 12-23)1. The pharmaceutical company is not liable for the damage caused by the data breach, as it can prove that it is not in any way responsible for the event giving rise to the damage. The company provided privacy training to Jack, informed him of the privacy policy, obtained his consent, and dismissed him as soon as the breach was discovered.Therefore, the company complied with the obligations of the GDPR, such as the accountability principle (Article 5 (2)), the data protection by design and by default principle (Article 25), the security of processing principle (Article 32), and the notification of a personal data breach to the supervisory authority principle (Article 33)1. Therefore, option D is the correct answer.Reference:Art. 82 GDPR -- Right to compensation and liability,Article 82 GDPR - GDPRhub

Question 3

Question Type: **MultipleChoice**

In the Planet 49 case, what was the man judgement of the Coon of Justice of the European Union (CJEU) regarding the issue of cookies?

Options:

A- If the cookies do not track personal data, then pre-checked boxes are acceptable.

B- If the ePrivacy Directive requires consent for cookies, then the GDPR's consent requirements apply.

C- If a website's cookie notice makes clear the information gathered and the lifespan of the cookie, then pre-checked boxes are acceptable.

D- If a data subject continues to scroll through a website after reading a cookie banner, this activity constitutes valid consent for the tracking described in the cookie banner.

Answer:

B

Explanation:

According to the CJEU, the ePrivacy Directive does not define the concept of consent, but refers to the GDPR for its interpretation1. Therefore, the GDPR standard of consent applies to the use of cookies and similar technologies that require consent under the ePrivacy Directive.The GDPR defines consent as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her2.The CJEU also clarified that the consent requirements apply regardless of whether the cookies constitute personal data or not, as the ePrivacy Directive covers any information stored or accessed on the user's device1.The other options are incorrect, as the CJEU ruled that pre-checked boxes, implicit consent by scrolling, and insufficient information on the cookies do not meet the GDPR standard of consent1.Reference:

Free CIPP/E Study Guide, page 14, section 2.3

GDPR, Article 4 (11)

ePrivacy Directive, Article 5 (3)

Planet49: CJEU Rules on Cookie Consent

CURIA - List of results

Question 4

Question Type: MultipleChoice

The transparency principle is most directly related to which of the following rights?

Options:

A- Right to object

B- Right to be informed.

C- Right to be forgotten.

D- Right to restriction of processing.

Answer:

B

Explanation:

The transparency principle, as stated in Article 5(1)(a) of the GDPR, requires that personal data be processed lawfully, fairly and in a transparent manner in relation to the data subject. This principle is closely linked to the right to be informed, as specified in Articles 13 and 14 of the GDPR, which oblige the controller to provide the data subject with certain information about the processing of their personal data, such as the identity and contact details of the controller, the purposes and legal basis of the processing, the recipients or categories of recipients of the personal data, the existence of the data subject's rights, and the retention period or criteria for the personal data. The right to be informed aims to ensure that the data subject is aware of and can verify the lawfulness of the processing, and to enable them to exercise their rights effectively. Therefore, the transparency principle is most directly related to the right to be informed.Reference:

Article 5(1)(a) of the GDPR

Article 13 of the GDPR

Article 14 of the GDPR

IAPP CIPP/E Study Guide, page 31

Question 5

Question Type: MultipleChoice

Articles 13 and 14 of the GDPR provide details on the obligation of data controllers to inform data subjects when collecting personal dat

a. However, both articles specify an exemption for situations in which the data subject already has the information.

Which other situation would also exempt the data controller from this obligation under Article 14?

Options:

A- When providing the information would go against a police order.

B- When providing the information would involve a disproportionate effort

C- When the personal data was obtained through multiple source in the public domain

D- When the personal data was obtained 5 years before the entry into force of the GDPR

Answer:

B

Explanation:

According to Article 14 of the GDPR, the data controller must provide the data subject with certain information when collecting personal data from a source other than the data subject1.However, there are some exceptions to this obligation, such as when the data subject already has the information, or when the provision of such information proves impossible or would involve a disproportionate effort2.The latter exception may apply, for example, when the personal data are collected from a large number of sources, or when the personal data are processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes3.The data controller must take appropriate measures to protect the data subject's rights and interests, and make the information publicly available2.Reference:1: Art.14 GDPR -- Information to be provided where personal data have not been obtained from the data subject2: Article 14(5)(b) of the GDPR3: Recital 62 of the GDPR.

Question 6

Question Type: MultipleChoice

Which kind of privacy notice, originally advocated by the Article 29 Working Party, is commonly recommended tor Al-based technologies because of the way it provides processing information at specific points of data collection?

Options:

A- Privacy dashboard notice

B- Visualization notice.

C- Just-in-lime notice.

D- Layered notice.

Answer:

A

Explanation:

According to the Article 29 Working Party, a just-in-time notice is a type of privacy notice that provides processing information at specific points of data collection, such as when the user clicks on a certain feature or enters personal data1.This kind of notice is commonly recommended for AI-based technologies because it allows the user to receive relevant and timely information about the processing of their data, without being overwhelmed by lengthy and complex privacy statements1.A just-in-time notice can also be combined with other types of notices, such as layered notices or privacy dashboards, to provide a more comprehensive and user-friendly transparency framework1. Therefore, option C is the correct answer.Option A is incorrect because a privacy dashboard notice is a type of notice that provides the user with a centralised and interactive overview of the processing of their data, and allows them to manage their privacy settings and preferences1.Option B is incorrect because a visualization notice is a type of notice that uses graphical elements, such as icons, symbols, colours, or animations, to convey the processing information in a more intuitive and engaging way1.Option D is incorrect because a layered notice is a type of notice that provides the processing information in a hierarchical and modular way, starting with the most essential information and allowing the user to access more details if they wish1.Reference:

What's new in WP29's final guidelines on transparency?

Question 7

Question Type: MultipleChoice

A company has collected personal data tor direct marketing purpose on the basis of consent. It is now considering using this data to develop new products through analytics. What is the company first required to do?

Options:

A- Obtain specific consent for the new processing

B- Only inform the data subjects of the new purpose.

C- Proceed no further, as such repurposing is unlawful

D- Update the privacy notice upon which consent was given

Answer:

A

Explanation:

According to the GDPR, consent is one of the lawful bases for processing personal data1.Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her2.Therefore, consent must be specific to each purpose of processing and cannot be bundled with other purposes3.If a company wants to use personal data for a new purpose that is not compatible with the original purpose for which consent was given, it must obtain a new consent from the data subjects for the new processing4. Simply informing the data subjects of the new purpose or updating the privacy notice is not sufficient, as it does not imply the data subject's agreement to the new processing.Proceeding with the new processing without obtaining a new consent would be unlawful and could result in fines and sanctions5.Reference:

Free CIPP/E Study Guide, page 23, section 4.1.1

GDPR, Article 4 (11)

GDPR, Recital 32

GDPR, Article 6 (4)

GDPR, Article 83 (5) (a)

Question 8

Question Type: MultipleChoice

A news website based m (he United Slates reports primarily on North American events The website is accessible to any user regardless of location, as the website operator does not block connections from outside of the U.S. The website offers a pad subscription that requires the creation of a user account; this subscription can only be paid in U.S. dollars.

Which of the following explains why the website operator, who is the responsible for all processing related to account creation and subscriptions, is NOT required to comply with the GDPR?

Options:

A- Payments cannot be made in a European Union currency.

B- The controller does not have an establishment in the European Union.

C- The website is not available in several official languages of European Un on Member States

D- The website cannot block connections from outside the U.S. that use a Virtual Private Network (VPN) to simulate a US location.

Answer:

A

Explanation:

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not1. This means that the GDPR applies to any controller or processor that has a branch, office, subsidiary, or other stable arrangement in the EU, even if the data processing occurs outside the

EU.However, the GDPR also applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union1. This means that the GDPR applies to any controller or processor that targets or tracks EU data subjects, even if they do not have a presence in the EU. In this case, the website operator is not required to comply with the GDPR because it does not have an establishment in the EU (option B), and it does not offer goods or services or monitor the behaviour of EU data subjects. The website operator reports primarily on North American events, does not block connections from outside the U.S., and only accepts payments in U.S. dollars, which indicate that it does not intend to target or track EU data subjects. Therefore, option B is the correct answer.Reference:Art. 3 GDPR -- Territorial scope,Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), [What does territorial scope mean under the GDPR?]

Question 9

Question Type: MultipleChoice

MagicClean is a web-based service located in the United States that matches home cleaning services to customers. It otters its services exclusively in the United States It uses a processor located in France to optimize its dat

a. Is MagicClean subject to the GDPR?

Options:

A- Yes, because MagicClean is processing data in the EU

B- Yes. because MagicClean's data processing agreement with the French processor is an establishment in the EU

C- No, because MagicClean is located m the United States only.

D- No. because MagicClean is not offering services to EU data subjects.

Answer:

D

Explanation:

According to Article 3 of the GDPR, the regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. The regulation also applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services to such data subjects in the EU or the monitoring of their behaviour as far as their behaviour takes place within the EU. In this case, MagicClean is a controller not established in the EU, and it does not offer services to EU data subjects or monitor their behaviour. Therefore, MagicClean is not subject to the GDPR, even if it uses a processor located in France to optimize its data. The location of the processor does not determine the applicability of the GDPR, but the context of the activities of the controller or the processor and the relationship with the data subjects.Reference:

Article 3 of the GDPR

IAPP CIPP/E Study Guide, page 14

Question 10

Question Type: MultipleChoice

Which of the following is NOT exempt from the material scope of the GDPR. insofar as the processing of personal data is concerned?

Options:

A- A natural person in the course of a large-scale but purely personal or household activity.

B- A natural person processing data foe a small-scale, purely personal or household activity.

C- A natural person in the course of processing purely personal or household data on behalf of a spouse who is beyond the age of majority.

D- A natural person in the course of activity conducted purely tor a personally-owned sole proprietorship.

Answer:

A

Explanation:

The material scope of the GDPR is outlined in Article 21.The Regulation applies to 'processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.'1However, the Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity1.This exemption is meant to protect the privacy of individuals in their private sphere and to exclude activities that have no connection with a professional or commercial activity2.The exemption covers activities such as correspondence, social networking, online publication of photos or videos, and the use of online services for personal purposes2.However, the exemption does not apply if the processing of personal data affects the rights and freedoms of others, such as when the data is made accessible to an indefinite number of people3. Therefore, the processing of personal data by a natural person in the course of a large-scale but purely personal or household activity is not exempt from the material scope of the GDPR, as it may have an impact on the privacy of other individuals.The other options are exempt from the material scope of the GDPR, as they involve small-scale, purely personal or household activities that do not affect the rights and freedoms of others.Reference:1: Article 2 of the GDPR2: Recital 18 of the GDPR3: CJEU, Case C-101/01, Lindqvist, 2003.

Question 11

Question Type: MultipleChoice

Two companies, Gellcoat and Freifish, make plans to launch a co-branded product the prototype of which is called Gellifish 9090. The companies want to organize an event to introduce the new product, so they decide to share data from their client databases and come up with a list of people to invite. They agree on the content of the invitations and together build an app to gather feedback at the event.

In this scenario, Gellcoat and Freifish are considered to be?

Options:

A- Joint controllers with respect to the personal data related to the event and separate controllers for their other purposes.

B- Joint controllers for all purposes because they have merged their databases and their data is now jointly owned.

C- Separate controllers because pint controllers^ requires a written designation in a contract

D- Separate controllers and processors since they are each providing services to the other

Answer:

A

Explanation:

According to the EDPB guidelines on the concepts of controller and processor in the GDPR1, joint controllers are entities that jointly determine the purposes and means of the processing of personal data. Joint controllership can result from a common decision or from converging decisions that are necessary for the processing to take place. Joint controllers must have a transparent arrangement that sets out their respective roles and responsibilities, and must ensure that individuals can exercise their rights against each controller. In this scenario, Gellcoat and Freifish are joint controllers with respect to the personal data related to the event, because they both decided to share data from their client databases, to come up with a list of people to invite, to agree on the content of the invitations, and to build an app to gather feedback. These decisions are joint and inseparable, and they have a tangible impact on the determination of the purposes and means of the processing. However, Gellcoat and Freifish are separate controllers for their other purposes, such as maintaining their own client databases, marketing their own products, or complying with their own legal obligations. These purposes are

independent and separate from the joint purpose of organizing the event. Therefore, option A is the correct answer. Option B is incorrect because joint controllership does not depend on the merging of databases or the ownership of data, but on the joint determination of purposes and means. Option C is incorrect because joint controllership does not require a written designation in a contract, but can be inferred from the factual circumstances. Option D is incorrect because separate controllers and processors have different roles and responsibilities under the GDPR, and Gellcoat and Freifish do not act as processors for each other.Reference:

Guidelines 07/2020 on the concepts of controller and processor in the GDPR

What does it mean if you are joint controllers?

What's New in the EDPB's Draft Guidelines on Controllers and Processors under the GDPR

Question 12

Question Type: MultipleChoice

A dynamic Internet Protocol (IP) address is considered persona! data when it is combined with what?

Options:

A- Other data held by the processor.

B- Other data held by the controller

C- Other data held by recipients of the data.

D- Other data held by Internet Service Providers (ISPs).

Answer:

B

Explanation:

A dynamic IP address is a unique numerical label for a device on the internet that changes every time the device connects to the internet. A dynamic IP address by itself is not personal data, as it does not directly identify the person who owns or uses the device. However, a dynamic IP address can become personal data when it is combined with other data held by the controller, such as the web pages accessed by the device, the time and duration of the visit, the location of the device, or the user's preferences and interests. In this case, the controller can use the additional data to identify the data subject, either directly or indirectly, by linking the dynamic IP address to a specific person or a profile. This was confirmed by the Court of Justice of the European Union (CJEU) in the case of Breyer v Bundesrepublik Deutschland, where the CJEU ruled that a dynamic IP address registered by a website provider constitutes personal data in relation to that provider, where the latter has the legal means to obtain the identity of the data subject from the internet service provider (ISP) that assigned the dynamic IP address. Therefore, option B is the correct answer.Reference:Directive 95/46/EC,Directive 2002/58/EC,Breyer v Bundesrepublik Deutschland, Case C-582/14,Dynamic IP Addresses can be Personal Data