Number: CIPP-E
Passing Score: 800
Time Limit: 120
File Version: 12.0

Exam Code: CIPP-E
Exam Name: Certified Information Privacy Professional/Europe (CIPP/E)

Exam A

QUESTION 1
Under the GDPR, which essential pieces of information must be provided to data subjects before collecting their personal data?

A. The authority by which the controller is collecting the data and the third parties to whom the data will be sent.
B. The name/s of relevant government agencies involved and the steps needed for revising the data.
C. The identity and contact details of the controller and the reasons the data is being collected.
D. The contact information of the controller and a description of the retention policy.

Correct Answer: C
Section:
Explanation:
The GDPR requires that data subjects are provided with certain information when their personal data are collected, either from the data subject themselves or from another source12.This information includes, among other things, the identity and contact details of the controller (and, where applicable, of the controller's representative and the data protection officer), and the purposes of the processing for which the personal data are intended as well as the legal basis for the processing34.This information is necessary to ensure fair and transparent processing of personal data, and to enable data subjects to exercise their rights under the GDPR5. Therefore, option C is the correct answer, as it contains two of the essential pieces of information that must be provided to data subjects before collecting their personal data.Options A, B and D are incorrect, as they do not include all the required information or include information that is not mandatory.Reference:1: Article 13 of the GDPR2: Article 14 of the GDPR3: Article 13(1)(a) and of the GDPR4: Article 14(1)(a) and of the GDPR5: Recital 60 of the GDPR

QUESTION 2
Assuming that the "without undue delay" provision is followed, what is the time limit for complying with a data access request?

A. Within 40 days of receipt
B. Within 40 days of receipt, which may be extended by up to 40 additional days
C. Within one month of receipt, which may be extended by up to an additional month
D. Within one month of receipt, which may be extended by an additional two months

Correct Answer: D
Section:
Explanation:
:According to the GDPR, data controllers must respond to a data access request (also known as a subject access request or SAR) without undue delay and in any event within one month of receipt of the request. This time limit can be extended by a further two months if the request is complex or if the controller receives a number of requests from the same individual. However, the controller must still inform the individual within one month of receipt of the request and explain why the extension is necessary. The time limit is calculated from the day after the request is received (whether it is a working day or not) until the corresponding calendar date in the next month. If there is no corresponding calendar date, the deadline is the last day of the next month. If the deadline falls on a weekend or public holiday, the response must be provided on the next working day.Reference:
GDPR, Article 12(3)
ICO, Right of access1
ICO, Time limits for responding to data protection rights requests2

QUESTION 3
The GDPR requires controllers to supply data subjects with detailed information about the processing of their data. Where a controller obtains data directly from data subjects, which of the following items of information does NOT legally have to be supplied?

A. The recipients or categories of recipients.
B. The categories of personal data concerned.
C. The rights of access, erasure, restriction, and portability.

D. The right to lodge a complaint with a supervisory authority.

Correct Answer: B
Section:
Explanation:
According to Article 13 of the GDPR, when a controller obtains personal data directly from the data subject, the controller must provide the data subject with certain information about the processing of their 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, the period of storage, the rights of the data subject, the right to lodge a complaint, etc. However, the controller does not have to provide the data subject with the categories of personal data concerned, as this information is already known by the data subject, since they provided the data themselves. This is different from Article 14, which applies when the controller obtains personal data from a source other than the data subject, and requires the controller to inform the data subject of the categories of personal data concerned, as well as the source of the data.Reference:
Art. 13 GDPR - Information to be provided where personal data are collected from the data subject
Art. 14 GDPR - Information to be provided where personal data have not been obtained from the data subject
Article 13: Information to be provided where personal data are collected from the data subject - GDPR

QUESTION 4
According to Article 14 of the GDPR, how long does a controller have to provide a data subject with necessary privacy information, if that subject's personal data has been obtained from other sources?

A. As soon as possible after obtaining the personal data.
B. As soon as possible after the first communication with the data subject.
C. Within a reasonable period after obtaining the personal data, but no later than one month.
D. Within a reasonable period after obtaining the personal data, but no later than eight weeks.

Correct Answer: C
Section:
Explanation:
According to Article 14 of the GDPR, if the controller obtains personal data from other sources, such as third parties or publicly accessible sources, the controller must provide the data subject with the necessary privacy information, such as the identity and contact details of the controller, the purposes and legal basis of the processing, the categories of personal data concerned, the recipients or categories of recipients of the personal data, and the rights of the data subject. The controller must provide this information within a reasonable period after obtaining the personal data, but no later than one month, having regard to the specific circumstances in which the personal data are processed.However, there are some exceptions to this rule, such as if the data subject already has the information, if the provision of the information proves impossible or would involve a disproportionate effort, if the obtaining or disclosure of the data is expressly laid down by EU or member state law, or if the personal data must remain confidential subject to an obligation of professional secrecy12.Reference:
GDPR, Article 14
Free CIPP/E Study Guide, page 19, section 2.5.1
CIPP/E Certification, page 14, section 1.2.1
Art. 14 GDPR - Information to be provided where personal data have not been obtained from the data subject
Article 14 GDPR - GDPRhub

QUESTION 5
When would a data subject NOT be able to exercise the right to portability?

A. When the processing is necessary to perform a task in the exercise of authority vested in the controller.
B. When the processing is carried out pursuant to a contract with the data subject.
C. When the data was supplied to the controller by the data subject.
D. When the processing is based on consent.

Correct Answer: A
Section:
Explanation:
The right to data portability only applies when the processing is based on the data subject's consent or on a contract with the data subject12.Therefore, if the processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller, the right to data portability does not apply12.This is because the data subject does not have a direct influence on the purpose or the means of the processing in

such cases3.Reference:1: Article 20 of the GDPR2: Right to data portability | ICO3: The right to data portability (Article 20 of the GDPR)

QUESTION 6
In which of the following situations would an individual most likely to be able to withdraw her consent for processing?

A. When she is leaving her bank and moving to another bank.
B. When she has recently changed jobs and no longer works for the same company.
C. When she disagrees with a diagnosis her doctor has recorded on her records.
D. When she no longer wishes to be sent marketing materials from an organization.

Correct Answer: D
Section:
Explanation:
According to the GDPR, consent is one of the six lawful bases for processing personal data. 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 her. Consent can be withdrawn at any time, and the withdrawal of consent must be as easy as giving it. Therefore, an individual can withdraw her consent for processing when she no longer wishes to be sent marketing materials from an organization, as this is a clear indication of her wishes and does not affect the lawfulness of the processing based on consent before its withdrawal. The other situations are not related to consent, but to other lawful bases such as contract, legitimate interest or legal obligation.Reference:Free CIPP/E Study Guide, page 9;CIPP/E Certification, page 3; GDPR, Article 4(11), Article 6(1)(a), Article 7(3).

QUESTION 7
As a result of the European Court of Justice's ruling in the case of Google v. Spain, search engines outside the EEA are also likely to be subject to the Regulation's right to be forgotten. This holds true if the activities of an EU subsidiary and its U.S. parent are what?

A. Supervised by the same Data Protection Officer.
B. Consistent with Privacy Shield requirements
C. Bound by a standard contractual clause.
D. Inextricably linked in their businesses.

Correct Answer: D
Section:
Explanation:
According to the CIPP/E study guide, the Court of Justice of the European Union (CJEU) ruled in the case of Google Spain SL, Google Inc.v Agencia Espaola de Proteccin de Datos (AEPD), Mario Costeja Gonzlez1that an Internet search engine operator is responsible for the processing of personal data that appear on web pages published by third parties, and that such operator must comply with the EU data protection law when it has an establishment in the EU. The CJEU held that Google Spain and Google Inc. were inextricably linked in their businesses, since Google Spain promoted and sold advertising space offered by Google Inc., which oriented its activity towards the inhabitants of Spain. Therefore, Google Inc. was subject to the EU data protection law through its subsidiary Google Spain, even though the personal data processing was carried out by Google Inc. outside the EU.This implies that search engines outside the EEA are also likely to be subject to the Regulation's right to be forgotten if they have an establishment in the EU that is inextricably linked to their parent company.Reference:1: CIPP/E study guide, page 16;Google Spain v AEPD and Mario Costeja Gonzlez

QUESTION 8
A German data subject was the victim of an embarrassing prank 20 years ago. A newspaper website published an article about the prank at the time, and the article is still available on the newspaper's website. Unfortunately, the prank is the top search result when a user searches on the victim's name. The data subject requests that SearchCo delist this result. SearchCo agrees, and instructs its technology team to avoid scanning or indexing the article. What else must SearchCo do?

A. Notify the newspaper that its article it is delisting the article.
B. Fully erase the URL to the content, as opposed to delist which is mainly based on data subject's name.
C. Identify other controllers who are processing the same information and inform them of the delisting request.
D. Prevent the article from being listed in search results no matter what search terms are entered into the search engine.

Correct Answer: A
Section:
Explanation:
According to theEuropean Data Protection Law & Practicetextbook, page 326, "the CJEU held that the search engine operator is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful." However, the CJEU also stated that "the operator of the search engine as the person responsible for that processing must, at the latest on the occasion of the erasure from its list of results, disclose to the operator of the web page containing that information the fact that that web page will no longer appear in the search engine's results following a search made on the basis of the data subject's name." Therefore, SearchCo must notify the newspaper that it is delisting the article, as part of its obligation to respect the data subject's right to be forgotten.Reference:
European Data Protection Law & Practice, page 326
CJEU Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Espaola de Proteccin de Datos, Mario Costeja Gonzlez, paragraphs 88 and 93

QUESTION 9
What are the obligations of a processor that engages a sub-processor?

A. The processor must give the controller prior written notice and perform a preliminary audit of the sub- processor.
B. The processor must obtain the controller's specific written authorization and provide annual reports on the sub-processor's performance.
C. The processor must receive a written agreement that the sub-processor will be fully liable to the controller for the performance of its obligations in relation to the personal data concerned.
D. The processor must obtain the consent of the controller and ensure the sub-processor complies with data processing obligations that are equivalent to those that apply to the processor.

Correct Answer: D
Section:
Explanation:
According to Article 28(2) of the GDPR, the processor may not engage another processor (sub-processor) without the prior specific or general written authorization of the controller. In the case of general written authorization, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. Furthermore, Article 28(4) of the GDPR states that where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Therefore, the processor must ensure that the sub-processor complies with data processing obligations that are equivalent to those that apply to the processor.Reference:
Article 28 of the GDPR
European Data Protection Law & Practice textbook, Chapter 6: Data Processing Obligations, Section 6.3: Processor Obligations, Subsection 6.3.2: Sub-processors

QUESTION 10
What must be included in a written agreement between the controller and processor in relation to processing conducted on the controller's behalf?

A. An obligation on the processor to report any personal data breach to the controller within 72 hours.
B. An obligation on both parties to report any serious personal data breach to the supervisory authority.
C. An obligation on both parties to agree to a termination of the agreement if the other party is responsible for a personal data breach.
D. An obligation on the processor to assist the controller in complying with the controller's obligations to notify the supervisory authority about personal data breaches.

Correct Answer: D
Section:
Explanation:
According to Article 28(3)(f) of the GDPR, the written agreement between the controller and the processor must include an obligation on the processor to assist the controller in ensuring compliance with the controller's obligations pursuant to Articles 32 to 36 of the GDPR. These obligations include notifying the supervisory authority and the data subjects about personal data breaches, as well as conducting data protection impact assessments and consulting with the supervisory authority when required. The processor must assist the controller by taking appropriate technical and organisational measures, insofar as this is possible, and considering the nature of the processing and the information available to the processor.Reference:
GDPR Article 28(3)(f)
CIPP/E Textbook, Chapter 6, Section 6.2.2, page 154
Free CIPP/E Study Guide, page 18

QUESTION 11
To provide evidence of GDPR compliance, a company performs an internal audit. As a result, it finds a data base, password-protected, listing all the social network followers of the client.
Regarding the domain of the controller-processor relationships, how is this situation considered?

A. Compliant with the security principle, because the data base is password-protected.
B. Non-compliant, because the storage of the data exceeds the tasks contractually authorized by the controller.
C. Not applicable, because the data base is password protected, and therefore is not at risk of identifying any data subject.
D. Compliant with the storage limitation principle, so long as the internal auditor permanently deletes the data base.

Correct Answer: B
Section:
Explanation:
The GDPR requires that the processor only processes personal data on behalf of the controller and according to the controller's instructions12.The agreement between the controller and the processor must include provisions that ensure that the processor does not process personal data for any other purposes or in a manner that is inconsistent with the controller's instructions34.Therefore, if the processor stores personal data that is not necessary for the performance of the contract with the controller, such as the social network followers of the client, this is a breach of the GDPR and the processor may be fined2. The fact that the data base is password-protected does not affect the applicability of the GDPR or the security principle, as the data is still personal data that can identify data subjects.The storage limitation principle also requires that personal data be kept for no longer than is necessary for the purposes for which the personal data are processed, so deleting the data base after the audit does not make the situation compliant.Reference:1: Article 28 of the GDPR2: Guidelines 07/2020 on the concepts of controller and processor in the GDPR3: Understanding Controller-to-Processor Agreements - GDPR Advisor4: New Guidelines on Data Controllers and Processors: Time to Review Data Processing Agreements : Article 4 of the GDPR : Article 5 of the GDPR

QUESTION 12
There are three domains of security covered by Article 32 of the GDPR that apply to both the controller and the processor. These include all of the following EXCEPT?

A. Consent management and withdrawal.
B. Incident detection and response.
C. Preventative security.
D. Remedial security.

Correct Answer: A
Section:
Explanation:
A) Consent management and withdrawal.Comprehensive Explanation:Article 32 of the GDPR requires the controller and the processor to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. These measures should take into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risks of varying likelihood and severity for the rights and freedoms of natural persons. The three domains of security covered by Article 32 are:
Preventative security:This refers to the measures that aim to prevent or reduce the likelihood of security incidents, such as unauthorized or unlawful access, disclosure, alteration, loss or destruction of personal data. Examples of preventative security measures include encryption, pseudonymization, access control, firewalls, antivirus software, etc.
Incident detection and response:This refers to the measures that aim to detect, analyze, contain, eradicate and recover from security incidents, as well as to notify the relevant authorities and data subjects, and to document the facts and actions taken. Examples of incident detection and response measures include security monitoring, logging, auditing, incident response plans, breach notification procedures, etc.
Remedial security:This refers to the measures that aim to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, as well as to mitigate the adverse effects of security incidents on the data subjects. Examples of remedial security measures include backup, disaster recovery, business continuity, compensation, etc.
Consent management and withdrawal is not a domain of security covered by Article 32, but rather a requirement for the lawfulness of processing based on consent under Article 6(1)(a) and Article 7 of the GDPR. Consent management and withdrawal involves obtaining, recording, updating and revoking the consent of data subjects for specific purposes of processing, as well as informing them of their right to withdraw their consent at any time.Reference:Free CIPP/E Study Guide, page 35;CIPP/E Certification, page 17; GDPR, Article 32, Article 6(1)(a), Article 7.

QUESTION 13
In the event of a data breach, which type of information are data controllers NOT required to provide to either the supervisory authorities or the data subjects?

A. The predicted consequences of the breach.

B. The measures being taken to address the breach.
C. The type of security safeguards used to protect the data.
D. The contact details of the appropriate data protection officer.

Correct Answer: A
Section:
Explanation:
According to the CIPP/E study guide, Article 33 of the GDPR requires data controllers to notify the supervisory authority of a personal data breach without undue delay and, where feasible, not later than 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons1.Article 34 of the GDPR requires data controllers to communicate the personal data breach to the data subject without undue delay when the breach is likely to result in a high risk to the rights and freedoms of natural persons2.Both articles specify the minimum information that the data controller must provide to the supervisory authority and the data subject, which includes: the nature of the breach, the categories and approximate number of data subjects and personal data records concerned, the name and contact details of the data protection officer or other contact point, the likely consequences of the breach, and the measures taken or proposed to address the breach and mitigate its possible adverse effects12.However, neither article requires the data controller to disclose the type of security safeguards used to protect the data, as this information is not relevant for the purposes of notification and may even compromise the security of the data further3.Reference:1: CIPP/E study guide, page 84;Art. 33 GDPR;Guidelines 01/2021 on Examples regarding Data Breach Notification2: CIPP/E study guide, page 85; [Art. 34 GDPR];Guidelines 01/2021 on Examples regarding Data Breach Notification3:Personal Data Breach | European Data Protection Supervisor;What is a data breach and what do we have to do ... - European Commission.

QUESTION 14
In which case would a controller who has undertaken a DPIA most likely need to consult with a supervisory authority?

A. Where the DPIA identifies that personal data needs to be transferred to other countries outside of the EEA.
B. Where the DPIA identifies high risks to individuals' rights and freedoms that the controller can take steps to reduce.
C. Where the DPIA identifies that the processing being proposed collects the sensitive data of EU citizens.
D. Where the DPIA identifies risks that will require insurance for protecting its business interests.

Correct Answer: B
Section:
Explanation:
According to theFree CIPP/E Study Guide, page 14, "if the DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller shall consult the supervisory authority prior to the processing." This means that the controller must seek the advice of the supervisory authority when the DPIA identifies high risks that cannot be sufficiently reduced by the controller's own measures. The other options are not necessarily cases where the consultation is required, although they may trigger other obligations under the GDPR, such as obtaining a valid legal basis, providing adequate safeguards, or informing the data subjects.Reference:
Free CIPP/E Study Guide, page 14
GDPR, Article 36

QUESTION 15
According to the GDPR, what is the main task of a Data Protection Officer (DPO)?

A. To create and maintain records of processing activities.
B. To conduct Privacy Impact Assessments on behalf of the controller or processor.
C. To monitor compliance with other local or European data protection provisions.
D. To create procedures for notification of personal data breaches to competent supervisory authorities.

Correct Answer: B
Section:
Explanation:
According to Article 35 of the GDPR, the controller must carry out a data protection impact assessment (DPIA) prior to processing that is likely to result in a high risk to the rights and freedoms of natural persons. The DPIA is a process for assessing and mitigating the potential impact of the processing on the protection of personal data. The controller must seek the advice of the DPO, where designated, when carrying out a DPIA. The DPO can assist the controller in conducting the DPIA and ensuring its compliance with the GDPR requirements. The DPO can also monitor the performance of the DPIA and act as a contact point for the supervisory authority and the data

subjects.Reference:
Article 35 of the GDPR
European Data Protection Law & Practice textbook, Chapter 7: Data Protection Impact Assessment, Section 7.2: When is a DPIA required?, Subsection 7.2.1: The role of the DPO
Roles and Responsibilities of a Data Protection Officer

QUESTION 16
A U.S.-based online shop uses sophisticated software to track the browsing behavior of its European customers and predict future purchases. It also shares this information with third parties. Under the GDPR, what is the online shop's PRIMARY obligation while engaging in this kind of profiling?

A. It must solicit informed consent through a notice on its website
B. It must seek authorization from the European supervisory authorities
C. It must be able to demonstrate a prior business relationship with the customers
D. It must prove that it uses sufficient security safeguards to protect customer data

Correct Answer: A
Section:
Explanation:
The GDPR defines profiling as any form of automated processing of personal data to evaluate certain personal aspects relating to a natural person, such as their preferences, behaviour, or interests1.Profiling is subject to the general principles and rules of the GDPR, such as lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality2.The GDPR also provides specific rights for data subjects who are subject to profiling, such as the right to be informed, the right to access, the right to rectify, the right to object, and the right to not be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects on them3.
In the given scenario, the online shop is engaging in profiling by tracking the browsing behaviour of its European customers and predicting future purchases. It is also sharing this information with third parties, which may involve further processing of the personal data. Therefore, the online shop must comply with the GDPR requirements for profiling and ensure that it has a valid legal basis for the processing.According to Article 6 of the GDPR, there are six possible legal bases for processing personal data: consent, contract, legal obligation, vital interests, public interest, or legitimate interests4.However, not all of them are equally applicable or appropriate for profiling activities, especially when they involve sensitive or special categories of data, such as biometric, genetic, or health data, which require additional safeguards under Article 9 of the GDPR5.
In this case, the most relevant and suitable legal basis for the online shop's profiling is consent, which means that the data subject has given a clear and affirmative indication of their agreement to the processing of their personal data for one or more specific purposes6.Consent must be freely given, specific, informed, and unambiguous, and must be obtained before the processing begins7. The online shop must also inform the data subject about the nature and purpose of the profiling, the logic involved, the consequences, and the rights they have in relation to it. The online shop must also respect the data subject's right to withdraw their consent at any time and to object to the profiling.
Therefore, the online shop's primary obligation while engaging in this kind of profiling is to solicit informed consent through a notice on its website, which must be clear, concise, and easily accessible, and must not be bundled with other terms and conditions. The online shop must also provide a simple and effective mechanism for the data subject to give or revoke their consent, such as a checkbox, a slider, or a button. The online shop must also keep records of the consent obtained and be able to demonstrate that it has complied with the GDPR requirements for consent.
The other options (B, C, and D) are not the primary obligation for the online shop, as they are either irrelevant or insufficient for the GDPR compliance. Seeking authorization from the European supervisory authorities is not necessary, unless the online shop is involved in a cross-border processing that requires a prior consultation under Article 36 of the GDPR. Demonstrating a prior business relationship with the customers is not a valid legal basis for the profiling, as it does not imply consent or legitimate interests. Proving that it uses sufficient security safeguards to protect customer data is a general obligation for any processing of personal data, but it does not address the specific issues and risks of profiling, such as discrimination, manipulation, or loss of control.Reference:
1:What is automated individual decision-making and profiling?
2:Article 5 of the GDPR
3:Rights related to automated decision making including profiling
4: [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)]
5:Article 9 of the GDPR
6:Article 4 (11) of the GDPR
7:Article 7 of the GDPR
:Article 13 and 14 of the GDPR
:Article 21 of the GDPR
:Article 12 of the GDPR
: [Guidelines on consent under Regulation 2016/679]
:Article 24 of the GDPR

:Article 36 of the GDPR
: [Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679]
: [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf]
: [https://edpb.europa.eu/sites/edpb/files/files/file1/20171104_wp251rev01_en.pdf]

QUESTION 17
Which of the following would NOT be relevant when determining if a processing activity would be considered profiling?

A. If the processing is to be performed by a third-party vendor
B. If the processing involves data that is considered personal data
C. If the processing of the data is done through automated means
D. If the processing is used to predict the behavior of data subjects

Correct Answer: A
Section:
Explanation:
The GDPR defines profiling as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements12. Therefore, the relevant factors when determining if a processing activity would be considered profiling are:
whether the processing involves data that is considered personal data;
whether the processing of the data is done through automated means; and
whether the processing is used to predict the behavior of data subjects.
The identity of the processor, whether it is the controller or a third-party vendor, is not relevant for the definition of profiling.However, it may have implications for the accountability and responsibility of the parties involved, as well as the data protection rights of the data subjects34.Reference:CIPP/E Certification - International Association of Privacy Professionals,Free CIPP/E Study Guide - International Association of Privacy Professionals,GDPR - EUR-Lex,What is automated individual decision-making and profiling? | ICO,WP29 releases guidelines on profiling under the GDPR,UK: A Guide To GDPR Profiling And Automated Decision-Making - Mondaq

QUESTION 18
Under Article 21 of the GDPR, a controller must stop profiling when requested by a data subject, unless it can demonstrate compelling legitimate grounds that override the interests of the individual. In the Guidelines on Automated individual decision-making and Profiling, the WP 29 says the controller needs to do all of the following to demonstrate that it has such legitimate grounds EXCEPT?

A. Carry out an exercise that weighs the interests of the controller and the basis for the data subject's objection.
B. Consider the impact of the profiling on the data subject's interest, rights and freedoms.
C. Demonstrate that the profiling is for the purposes of direct marketing.
D. Consider the importance of the profiling to their particular objective.

Correct Answer: C
Section:
Explanation:
:According to the UK GDPR, the data subject has the right to object, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions1.The controller must stop the processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims1.The WP 29 Guidelines on Automated individual decision-making and Profiling provide some guidance on how to assess the existence of such compelling legitimate grounds2.The controller needs to carry out an exercise that weighs the interests of the controller and the basis for the data subject's objection, consider the impact of the profiling on the data subject's interest, rights and freedoms, and consider the importance of the profiling to their particular objective2.However, the controller does not need to demonstrate that the profiling is for the purposes of direct marketing, as this is a separate ground for objection under Article 21(2) of the UK GDPR, which gives the data subject an absolute right to object to such processing13.Therefore, option C is the correct answer, as it is not required by the controller to demonstrate that it has compelling legitimate grounds for profiling.Reference:132
https://gdpr.eu/article-21-right-to-object/ https://ico.org.uk/for-organisations-2/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

QUESTION 19
SCENARIO

Please use the following to answer the next question:
TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.
During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed Questionaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories -- age, income, ethnicity -- that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the Questionaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.
Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.
If TripBliss Inc. decides not to report the incident to the supervisory authority, what would be their BEST defense?

A. The resulting obligation to notify data subjects would involve disproportionate effort.
B. The incident resulted from the actions of a third-party that were beyond their control.
C. The destruction of the stolen data makes any risk to the affected data subjects unlikely.
D. The sensitivity of the categories of data involved in the incident was not substantial enough.

Correct Answer: C
Section:
Explanation:
According to the GDPR, data controllers must report personal data breaches to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it (Art 33 of GDPR). However, the notification is not required if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (Art 33(1) of GDPR). In this case, TripBliss Inc. could argue that the stolen data was securely erased by Leon before it could be disclosed to anyone else, and therefore the risk of harm to the data subjects was minimal. TripBliss Inc. would have to provide evidence of the secure deletion of the data and the absence of any copies or backups. Alternatively, TripBliss Inc. could also invoke the exception of disproportionate effort to avoid notifying the data subjects directly, but only if they have made a public communication or similar measure to inform them in an equally effective manner (Art 34(3)(b) of GDPR). The other options are not valid defenses, as they do not affect the likelihood of risk to the data subjects. The incident was not caused by a third-party, but by an employee of Techiva, who was acting as a data processor on behalf of TripBliss Inc. As the data controller, TripBliss Inc. is responsible for ensuring that the data processor provides sufficient guarantees to implement appropriate technical and organisational measures to comply with the GDPR (Art 28 of GDPR). The sensitivity of the data categories is not relevant for the notification obligation, as any personal data breach could pose a risk to the data subjects, depending on the circumstances. The GDPR does not provide a threshold for the sensitivity of the data, but rather requires a case-by-case assessment of the potential impact of the breach.Reference:
GDPR, Art 33, Art 34, Art 28
Free CIPP/E Study Guide, p. 15
European Data Protection Law & Practice, p. 123-124
Personal data breach notification under the GDPR

QUESTION 20
SCENARIO
Please use the following to answer the next question:
TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.
During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed Questionaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories -- age, income, ethnicity -- that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the Questionaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.

Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.
With regard to TripBliss Inc.'s use of website cookies, which of the following statements is correct?

A. Because not all of the cookies are strictly necessary to enable the use of a service requested from TripBliss Inc., consent requirements apply to their use of cookies.
B. Because of the categories of data involved, explicit consent for the use of cookies must be obtained separately from customers.
C. Because Techiva will receive only aggregate statistics of data collected from the cookies, no additional consent is necessary.
D. Because the use of cookies involves the potential for location tracking, explicit consent must be obtained from customers.

Correct Answer: A
Section:
Explanation:
According to the ePrivacy Directive (2002/58/EC), the use of cookies or similar devices that store or access information on the user's device requires the user's consent, unless the cookie is strictly necessary to enable the use of a service requested by the user. For example, a cookie that remembers the items in a shopping cart does not require consent, but a cookie that tracks the user's browsing behavior for analytics or advertising purposes does. The consent must be freely given, specific, informed, and unambiguous, and can be obtained through appropriate settings of the browser or other application. The consent must also be separate from other consents, such as the consent to the processing of personal data. The categories of data involved or the recipients of the data do not affect the consent requirement for the use of cookies. The consent must also be obtained before the cookie is placed or accessed, unless the cookie is exempted. Therefore, option A is correct.
Option B is incorrect because explicit consent is not required for the use of cookies, unless the cookie also involves the processing of special categories of personal data under the GDPR. However, in this scenario, there is no indication that the cookies collect or process such data. Therefore, option B is incorrect.
Option C is incorrect because the consent requirement for the use of cookies does not depend on the recipients of the data or the level of aggregation of the data. The consent must be obtained from the user whose device is accessed or stored by the cookie, regardless of who receives the data or how it is processed. Therefore, option C is incorrect.
Option D is incorrect because the consent requirement for the use of cookies does not depend on the potential for location tracking. The consent must be obtained for any cookie that is not strictly necessary to enable the use of a service requested by the user, regardless of the type or purpose of the cookie. Therefore, option D is incorrect.
ePrivacy Directive, Article 5(3)
GDPR, Article 4(11), Article 7, Article 9
CIPP/E Study Guide, Chapter 5, Section 5.2.2

QUESTION 21
Company X has entrusted the processing of their payroll data to Provider Y. Provider Y stores this encrypted data on its server. The IT department of Provider Y finds out that someone managed to hack into the system and take a copy of the data from its server. In this scenario, whom does Provider Y have the obligation to notify?

A. The public
B. Company X
C. Law enforcement
D. The supervisory authority

Correct Answer: B
Section:
Explanation:
According to Article 33 of the GDPR, in the case of a personal data breach, the processor (Provider Y) shall notify the controller (Company X) without undue delay after becoming aware of the breach. The processor does not have the obligation to notify the supervisory authority, the public, or law enforcement, unless otherwise required by law. The controller is responsible for notifying the supervisory authority and, where necessary, the data subjects, unless the breach is unlikely to result in a risk to their rights and freedoms.Reference:
Article 33 of the GDPR, which regulates the notification of a personal data breach to the supervisory authority.
[Article 34 of the GDPR], which regulates the communication of a personal data breach to the data subject.
ICO guidance, which explains the roles and responsibilities of controllers and processors in relation to data breach notification.

QUESTION 22
When hiring a data processor, which action would a data controller NOT be able to depend upon to avoid liability in the event of a security breach?

A. Documenting due diligence steps taken in the pre-contractual stage.
B. Conducting a risk assessment to analyze possible outsourcing threats.
C. Requiring that the processor directly notify the appropriate supervisory authority.
D. Maintaining evidence that the processor was the best possible market choice available.

Correct Answer: C
Section:
Explanation:
The GDPR imposes several obligations on data controllers when they engage data processors to process personal data on their behalf.One of these obligations is to ensure that the contract or other legal act between the controller and the processor stipulates that the processor must assist the controller in complying with its obligations under the GDPR, including the obligation to notify personal data breaches to the competent supervisory authority and, where applicable, to the affected data subjects1. However, this does not mean that the processor can directly notify the supervisory authority without the involvement of the controller.The GDPR clearly states that it is the controller's responsibility to notify the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of the breach2.The processor must only notify the controller without undue delay after becoming aware of the breach3. Therefore, requiring that the processor directly notify the appropriate supervisory authority is not an action that a data controller can depend upon to avoid liability in the event of a security breach, as it would be contrary to the GDPR and the controller's own obligation.Options A, B and D are actions that a data controller can take to reduce the risk of liability, as they demonstrate that the controller has exercised due diligence, assessed the potential impact of outsourcing, and chosen a reliable and compliant processor.Reference:1: Article 28(3)(f) of the GDPR2: Article 33(1) of the GDPR3: Article 33(2) of the GDPR

QUESTION 23
WP29's "Guidelines on Personal data breach notification under Regulation 2016/679" provides examples of ways to communicate data breaches transparently. Which of the following was listed as a method that would NOT be effective for communicating a breach to data subjects?

A. A postal notification
B. A direct electronic message
C. A notice on a corporate blog
D. A prominent advertisement in print media

Correct Answer: C
Section:
Explanation:
According to the WP29's "Guidelines on Personal data breach notification under Regulation 2016/679'', the communication of a personal data breach to the data subjects should be clear, concise, transparent, easily accessible and understandable, and use clear and plain language. The communication should also be made as soon as reasonably feasible and in close cooperation with the supervisory authority. The guidelines provide some examples of methods that may be effective for communicating a breach to data subjects, such as a direct electronic message (e.g. email, SMS, direct message), a postal notification, a prominent advertisement in print media, or a notice on the homepage of the affected website. However, the guidelines also state that a notice on a corporate blog or social media would not be an effective method of communication, as it would not reach all the affected data subjects and would not allow them to take immediate action to protect themselves. Therefore, the correct answer is C. A notice on a corporate blog.Reference:
WP29's "Guidelines on Personal data breach notification under Regulation 2016/679'', pages 20-211

QUESTION 24
Which of the following would require designating a data protection officer?

A. Processing is carried out by an organization employing 250 persons or more.
B. Processing is carried out for the purpose of providing for-profit goods or services to individuals in the EU.
C. The core activities of the controller or processor consist of processing operations of financial information or information relating to children.
D. The core activities of the controller or processor consist of processing operations that require systematic monitoring of data subjects on a large scale.

Correct Answer: D

Section:
Explanation:
According to Article 37 of the GDPR, the designation of a data protection officer (DPO) is mandatory for controllers and processors in three cases1:
When the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
When the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
When the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
The GDPR does not define what constitutes "regular and systematic monitoring" or "large scale'', but the Article 29 Working Party (now replaced by the European Data Protection Board) has provided some guidance on these concepts2. According to the guidance, "regular and systematic monitoring" includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising, but also offline activities such as CCTV or health data monitoring. The guidance also suggests some criteria to assess whether the processing is carried out on a large scale, such as the number of data subjects concerned, the volume of data or the range of data items processed, the duration or permanence of the processing activity, and the geographical extent of the processing.
In the given scenario, option D is the only one that clearly falls under the second case of mandatory DPO designation, as it implies that the controller or processor is engaged in regular and systematic monitoring of data subjects on a large scale as part of their core activities. This could include, for example, online behavioural advertising, location tracking, loyalty programs, or health data analytics. The other options are not sufficient to trigger the obligation to appoint a DPO, unless they are combined with other factors that indicate a large scale or a high risk of the processing. For instance, option A is not relevant, as the GDPR does not set a threshold based on the size or number of employees of the organisation. Option B is also not decisive, as the GDPR does not distinguish between for-profit or non-profit purposes of the processing. Option C may require a DPO if the processing of financial information or information relating to children is done on a large scale and involves special categories of data, but it is not a general rule.Reference:
1:Article 37 of the GDPR
2:Guidelines on Data Protection Officers ('DPOs')
3: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)
4:https://edpb.europa.eu/sites/edpb/files/files/file1/wp243rev01_en.pdf
5:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
6: [https://edpb.europa.eu/sites/edpb/files/files/file1/wp243rev01_en.pdf]
7: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679]

QUESTION 25
Which statement is correct when considering the right to privacy under Article 8 of the European Convention on Human Rights (ECHR)?

A. The right to privacy is an absolute right
B. The right to privacy has to be balanced against other rights under the ECHR
C. The right to freedom of expression under Article 10 of the ECHR will always override the right to privacy
D. The right to privacy protects the right to hold opinions and to receive and impart ideas without interference

Correct Answer: B
Section:
Explanation:
Article 8 of the ECHR protects the right to respect for private and family life, home and correspondence. However, this right is not absolute and can be subject to limitations by a public authority in accordance with the law and for a legitimate aim. The European Court of Human Rights (ECtHR) has developed a two-stage test to determine whether such limitations are justified. First, the court must examine whether there is a legitimate aim pursued by the public authority, such as national security, public safety or the prevention of crime.Second, the court must assess whether the means used by the public authority are appropriate and necessary to achieve that aim, taking into account all relevant factors such as proportionality, necessity and less restrictive alternatives12. Therefore, the right to privacy is not an absolute right but a qualified one that has to be balanced against other rights under the ECHR.Reference:
Article 8 - Protection of personal data
Your right to respect for private and family life
Right to respect for private and family life
Guide on Article 8 of the European Convention on Human Rights
European Convention on Human Rights - Article 8

QUESTION 26

What is one major goal that the OECD Guidelines, Convention 108 and the Data Protection Directive (Directive 95/46/EC) all had in common but largely failed to achieve in Europe?

A. The establishment of a list of legitimate data processing criteria
B. The creation of legally binding data protection principles
C. The synchronization of approaches to data protection
D. The restriction of cross-border data flow

Correct Answer: C
Section:
Explanation:
The OECD Guidelines, Convention 108 and the Data Protection Directive (Directive 95/46/EC) all aimed to harmonize the national data protection laws of the member states of the European Economic Community (EEC) and to establish a common framework for the protection of personal data. However, they largely failed to achieve this goal due to several reasons, such as:
The lack of political will and commitment from the member states to implement the directives fully and consistently12.
The divergent interpretations and applications of the directives by different national authorities, courts and regulators12.
The emergence of new technologies and challenges that required new or updated legal solutions, such as electronic communications, cookies, biometrics, cloud computing, etc12.
The influence of other regional or international initiatives that addressed some aspects of data protection differently or in conflict with the directives, such as the US Privacy Shield Framework3.

QUESTION 27
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?

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

Correct Answer: D
Section:
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 28
Which EU institution is vested with the competence to propose new data protection legislation on its own initiative?

A. The European Council
B. The European Parliament

C. The European Commission
D. The Council of the European Union

Correct Answer: C
Section:
Explanation:
According to the CIPP/E study guide1, the European Commission is the EU institution that has the power to propose new data protection legislation on its own initiative, as well as amend or repeal existing laws. The European Commission is also responsible for implementing and enforcing the EU data protection framework, in cooperation with other institutions and national authorities.

QUESTION 29
What is an important difference between the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU) in relation to their roles and functions?

A. ECHR can rule on issues concerning privacy as a fundamental right, while the CJEU cannot.
B. CJEU can force national governments to implement and honor EU law, while the ECHR cannot.
C. CJEU can hear appeals on human rights decisions made by national courts, while the ECHR cannot.
D. ECHR can enforce human rights laws against governments that fail to implement them, while the CJEU cannot.

Correct Answer: B
Section:
Explanation:
The ECHR and the CJEU are part of two different legal systems: the Council of Europe and the European Union, respectively. The ECHR is a treaty that guarantees human rights and fundamental freedoms to individuals within the jurisdiction of its 47 member states. The CJEU is the judicial branch of the EU that ensures the uniform interpretation and application of EU law within its 27 member states. The ECHR can only hear complaints from individuals or states alleging violations of the rights enshrined in the convention, and it can only issue judgments that are binding on the respondent state. The CJEU, on the other hand, can hear cases from individuals, states, EU institutions, or national courts on any matter of EU law, and it can issue rulings that are binding on all EU member states and institutions. The CJEU can also impose sanctions or penalties on states that fail to comply with its judgments or EU law in general. Therefore, the CJEU has more power and authority to enforce EU law than the ECHR has to enforce human rights law.Reference:CIPP/E Certification,ECHR and the CJEU,The UK, the EU and a British Bill of Rights

QUESTION 30
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.
Which of the University's records does Anna NOT have to include in her record of processing activities?

A. Student records

B. Staff and alumni records
C. Frank's performance database
D. Department for Education records

Correct Answer: C
Section:
Explanation:
According to the GDPR, a record of processing activities (RoPA) is a document that provides an overview of how personal data is processed within an organisation.It must include information on the types of personal data processed, the purposes for which the data is processed, and the measures taken to ensure the security of the data123.A RoPA must be kept up to date and made available to the supervisory authority upon request1.
In this scenario, Anna does not have to include Frank's performance database in her RoPA, because it does not contain any personal data.Personal data is any information relating to an identified or identifiable natural person4. Frank's performance database only contains aggregated or anonymised data that cannot identify any individual student. Therefore, it does not fall under the definition of personal data under the GDPR.
However, Anna still has to complete her RoPA for all other types of records that are processed by Granchester University, such as student records, staff and alumni records, and Department for Education records.These records may contain personal data that needs to be minimised and protected in accordance with the GDPR principles4.Anna also has to conduct a risk analysis before processing these records, as required by Article 35(2) of the GDPR4.She also has to report any security incidents involving these records, as required by Article 33(3) of the GDPR4.
[Art. 30 GDPR -- Records of processing activities]
[How do we document our processing activities?]
Records of Processing (Article 30) Guidance
GDPR Records of Processing Activities | Resources
Records of Processing Activities: A Key GDPR Compliance Requirement

QUESTION 31
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.
Before Anna determines whether Frank's performance database is permissible, what additional information does she need?

A. More information about Frank's data protection training.
B. More information about the extent of the information loss.
C. More information about the algorithm Frank used to mask student numbers.
D. More information about what students have been told and how the research will be used.

Correct Answer: D
Section:
Explanation:

Before Anna determines whether Frank's performance database is permissible, she needs to know more information about the following aspects of the data processing:
The purpose and legal basis of the data processing, which should be clearly defined and documented in a data protection impact assessment (DPIA) or a similar document12.
The nature and extent of the personal data involved, which should be limited to what is necessary for the purpose and not retained longer than necessary12.
The measures taken to ensure the security and confidentiality of the personal data, such as encryption, pseudonymization, access control, etc12.
The rights and interests of the data subjects, such as their right to access, rectify, erase or restrict their personal data, as well as their right to object or withdraw consent12.
The potential risks and consequences of the data processing for the rights and freedoms of the data subjects, such as identity theft, discrimination, reputational damage, etc12.
In this case, Anna needs to know more information about what students have been told and how the research will be used. This is because:
The purpose of using student records for research purposes is not clear from Frank's description. He does not specify whether he has obtained consent from the students or their parents/guardians, or whether he has informed them about his research objectives and methods.
The nature and extent of using student records for research purposes is not clear from Frank's description. He does not specify which student records he is using (e.g., by name or by reference number), how many records he is using (e.g., by cohort or by class), or how long he will keep them (e.g., until graduation or indefinitely).
The measures taken to ensure the security and confidentiality of using student records for research purposes are not clear from Frank's description. He does not specify whether he has encrypted his program or his laptop before transferring it to his home device, whether he has backed up his program or his laptop before losing it on the train, or whether he has reported his lost laptop to his IT department.
Therefore, Anna needs more information about these aspects before she can determine whether Frank's performance database is permissible under the GDPR.

QUESTION 32
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?

A. The data subjects are no longer current students of Frank's
B. The processing will not negatively affect the rights of the data subjects
C. The algorithms that Frank uses for the processing are technologically sound
D. The data subjects gave their unambiguous consent for the original processing

Correct Answer: A
Section:
Explanation:
A risk analysis is a process of identifying, assessing and mitigating the potential threats and vulnerabilities that may affect the personal data processing activities of an organization. A risk analysis is not a one-time activity, but a continuous and dynamic process that requires regular monitoring and updating. A risk analysis is also not a substitute for compliance with the GDPR, but a tool to help ensure compliance by identifying and addressing the legal obligations and best practices.
According to the GDPR, an organization must conduct a data protection impact assessment (DPIA) before starting any new or significantly increased processing activity that may pose a high risk to the rights and freedoms of the data subjects. A DPIA is a systematic and documented process that aims to identify, evaluate and mitigate the risks associated with such processing activities. A DPIA must be carried out by or on behalf of the controller

(the person or entity that determines the purposes and means of processing) or by another person acting on their behalf.
In this scenario, Frank is conducting a DPIA for his new processing activity of analyzing his students' performance data in relation to Department for Education expectations. This processing activity poses a high risk to the rights and freedoms of his students, as it involves collecting, storing, using and transferring their personal data without their explicit consent or knowledge. Therefore, Frank must conduct a DPIA before starting this processing activity.
However, there are some exceptions to this requirement. One of them is when the processing activity involves personal data that are no longer relevant for the original purpose for which they were collected or otherwise processed. In this case, Frank can use existing personal data without conducting a DPIA, as long as he ensures that they are adequate, relevant and limited to what is necessary for his new purpose.
Therefore, in this situation, 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. This means that Frank can use his existing student records without conducting a DPIA, as long as he ensures that they are adequate, relevant and limited to what is necessary for his new purpose.
Risks and data protection impact assessments (DPIAs) | ICO
What Are GDPR Risk Assessments and Why Are They Important?
GDPR Compliance Risk Assessment Best Practices | Accountable
Why risk assessments are essential for GDPR compliance

QUESTION 33
Which institution has the power to adopt findings that confirm the adequacy of the data protection level in a non-EU country?

A. The European Parliament
B. The European Commission
C. The Article 29 Working Party
D. The European Council

Correct Answer: B
Section:
Explanation:
According to Article 45 of the GDPR, the European Commission has the power to determine, on the basis of an assessment, whether a non-EU country, a territory or a sector within that country, or an international organisation ensures an adequate level of data protection. This means that the data protection rules and standards in that country or organisation are equivalent to those in the EU. The effect of an adequacy decision is that personal data can flow freely from the EU to that country or organisation without any further safeguards or authorisations. The European Commission has adopted adequacy decisions for several countries and organisations, such as Japan, Canada, and the EU-US Data Privacy Framework.Reference:Data protection adequacy for non-EU countries,Adequate Level of Protection

QUESTION 34
What is true of both the General Data Protection Regulation (GDPR) and the Council of Europe Convention 108?

A. Both govern international transfers of personal data
B. Both govern the manual processing of personal data
C. Both only apply to European Union countries
D. Both require notification of processing activities to a supervisory authority

Correct Answer: D
Section:
Explanation:
The GDPR and the Convention 108 are two important data protection instruments that aim to protect the rights and freedoms of individuals with regard to their personal data. They both have some similarities and some differences, but one common feature is that they both require notification of processing activities to a supervisory authority.
A supervisory authority is an independent public body that monitors and enforces compliance with data protection laws.In the EU, there are 47 national data protection authorities (DPAs) that have the power to impose administrative fines, issue guidelines, conduct investigations, and cooperate with other authorities1.In the Council of Europe, there are 54 parties to the Convention 108 that have established their own supervisory authorities or have agreed to be supervised by an external authority2.
Notification of processing activities is a requirement for any controller or processor of personal data that falls under the scope of the GDPR or the Convention 108.A controller is a natural or legal person who determines the purposes and means of the processing of personal data3.A processor is a natural or legal person who processes personal data on behalf of a controller3. Notification means informing the supervisory authority about certain aspects of the processing, such as:
The identity and contact details of the controller and processor

The categories and sources of personal data
The purposes and legal basis for processing
The recipients or categories of recipients of personal data
The retention period or criteria for determining it
The existence of any automated decision-making or profiling
The rights of data subjects and how they can exercise them
Notification can be done in various ways, such as:
Submitting a written notification form
Publishing a notice on a website or other platform
Sending an email or other electronic message
Using an online system or portal
Notification should be done as soon as possible after becoming aware of any relevant information about the processing.It should also be updated whenever there are significant changes in relation to the processing4.
Therefore, both the GDPR and the Convention 108 require notification of processing activities to a supervisory authority. This is one way to ensure transparency, accountability, and compliance with data protection laws.

QUESTION 35
Which aspect of the GDPR will likely have the most impact on the consistent implementation of data protection laws throughout the European Union?

A. That it essentially functions as a one-stop shop mechanism
B. That it takes the form of a Regulation as opposed to a Directive
C. That it makes notification of large-scale data breaches mandatory
D. That it makes appointment of a data protection officer mandatory

Correct Answer: B
Section:
Explanation:
One of the main differences between a Regulation and a Directive in the EU law is that a Regulation is directly applicable and binding in all EU member states, without the need for national implementing measures, while a Directive sets out the objectives and principles that the member states must achieve, but leaves them the choice of form and methods to transpose it into their national laws. Therefore, by taking the form of a Regulation, the GDPR aims to harmonize and unify the data protection rules across the EU, and to ensure a consistent implementation and enforcement of the data protection laws throughout the EU. The other aspects of the GDPR listed in the question, such as the one-stop shop mechanism, the mandatory notification of large-scale data breaches, and the mandatory appointment of a data protection officer, are also important features of the GDPR, but they do not have the same impact on the consistency of the data protection laws as the form of a Regulation.

QUESTION 36
How is the retention of communications traffic data for law enforcement purposes addressed by European data protection law?

A. The ePrivacy Directive allows individual EU member states to engage in such data retention.
B. The ePrivacy Directive harmonizes EU member states' rules concerning such data retention.
C. The Data Retention Directive's annulment makes such data retention now permissible.
D. The GDPR allows the retention of such data for the prevention, investigation, detection or prosecution of criminal offences only.

Correct Answer: B
Section:
Explanation:
The ePrivacy Directive is a European Union (EU) directive that aims to protect the confidentiality of electronic communications and prevent their indiscriminate interception or monitoring. It was adopted in 2002 and amended in 2009.It applies to all providers of electronic communication services, such as internet service providers, mobile network operators, and online platforms12.
One of the main objectives of the ePrivacy Directive is to ensure that the retention of communications traffic data for law enforcement purposes is subject to strict conditions and safeguards.Communications traffic data refers to any information relating to the transmission or routing of electronic communications, such as IP addresses, timestamps, and metadata3.Such data can be used by competent national authorities for the prevention, investigation, detection or prosecution of criminal offences and safeguarding national security4.
However, the ePrivacy Directive does not allow individual EU member states to engage in such data retention without harmonizing their rules. Article 6(1)(b) of the directive states that "Member States shall ensure that any measures taken by them in relation to the retention of traffic data are consistent with this Directive''.Therefore, each EU member state must adopt a national law that complies with the requirements and limitations set by the

directive12.
The Data Retention Directive (DRD) was a previous EU directive that aimed to establish a common framework for the retention of communications traffic data for law enforcement purposes across all EU member states. It was adopted in 2006 and amended in 2010. However, it was annulled by the Court of Justice of the European Union (CJEU) in 2014 on procedural grounds.The CJEU found that some provisions of the DRD were inconsistent with other EU directives and principles, such as Article 8(2) of the Charter of Fundamental Rights (CFR), which protects individuals from arbitrary interference with their privacy56.
The GDPR is a new EU regulation that implements some aspects of the DRD into national law through its provisions on processing personal data. However, it does not address directly the issue of communications traffic data retention for law enforcement purposes. Instead, it requires providers to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved in processing personal data.These measures include encryption, pseudonymisation, access control, and accountability7.The GDPR also grants individuals certain rights regarding their personal data, such as access, rectification, erasure, portability, and objection7.
Therefore, under current EU law, there is no single legal basis for retaining communications traffic data for law enforcement purposes across all EU member states. Each member state must adopt its own national law that respects the principles and limitations established by the ePrivacy Directive.
ePrivacy Directive
ePrivacy Regulation
What is Communications Traffic Data?
How is Communications Traffic Data Retained?
Data Retention Directive
Data Retention Directive annulled by CJEU
General Data Protection Regulation
What are your rights regarding your personal data?

QUESTION 37
What type of data lies beyond the scope of the General Data Protection Regulation?

A. Pseudonymized
B. Anonymized
C. Encrypted
D. Masked

Correct Answer: B
Section:
Explanation:
:The General Data Protection Regulation (GDPR) is a data protection law that applies to the processing of personal data of individuals in the European Union (EU) and the European Economic Area (EEA).Personal data is any information relating to an identified or identifiable natural person, such as name, address, email, phone number, etc12.The GDPR does not apply to personal data that is anonymized, meaning that it cannot be linked back to a specific individual12.Anonymization can be achieved by removing or masking any identifying information from the data, such as using pseudonyms, aggregating or generalizing the data, or applying statistical methods12.
Therefore, the type of data that lies beyond the scope of the GDPR is anonymized data.
https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en#:~:text=Different%20pieces%20of%20information%2C%20which,the%20scope%20of%20the%20GDPR. B. ANONYMIZED
Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the GDPR. Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

QUESTION 38
Under what circumstances would the GDPR apply to personal data that exists in physical form, such as information contained in notebooks or hard copy files?

A. Only where the personal data is produced as a physical output of specific automated processing activities, such as printing, labelling, or stamping.
B. Only where the personal data is to be subjected to specific computerized processing, such as image scanning or optical character recognition.
C. Only where the personal data is treated by automated means in some way, such as computerized distribution or filing.
D. Only where the personal data is handled in a sufficiently structured manner so as to form part of a filing system.

Correct Answer: D
Section:

Explanation:
The GDPR applies to all personal data, regardless of whether it exists in physical form or not.The GDPR defines personal data as any information relating to an identified or identifiable natural person, such as names, identification numbers, location data, or online identifiers1. Therefore, any information that can be linked directly or indirectly to a natural person is considered personal data under the GDPR.
However, the GDPR also distinguishes between different types of processing activities and their legal bases. Processing activities are the operations performed on personal data, such as collection, storage, use, disclosure, or deletion. Processing activities can be either automated or manual. Automated processing means using technology to perform processing activities without human intervention. Manual processing means using human intervention to perform processing activities.
The GDPR requires that any processing activity that involves personal data must comply with certain principles and conditions, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality. These principles and conditions apply to both automated and manual processing activities.
Therefore, the GDPR applies to personal data that exists in physical form only when it is processed by an automated means in some way that affects its rights and freedoms. For example, if a company scans paper documents and stores them electronically in a database without deleting them after a certain period of time or when they are no longer needed for the original purpose for which they were collected (Article 6), then this would be considered an automated processing activity that involves personal data in physical form.
However, the GDPR does not apply to personal data that exists in physical form when it is handled in a sufficiently structured manner so as to form part of a filing system. For example, if a company keeps paper documents in folders labeled with names and dates on their office shelves without scanning them or storing them electronically anywhere else (Article 5), then this would not be considered an automated processing activity that involves personal data in physical form.
Physical Data - GDPR Summary
What GDPR Means for Your Physical Records - Access
Personal Data - Data Protection Act 2018

QUESTION 39
SCENARIO
Please use the following to answer the next question:
You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and Asia. A large portion of the company's revenue is due to international sales.
The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered: The figures can answer children's Questions: on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well. The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.
When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's question. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.
In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a Near-Field Communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of the home and have the character's abilities remain intact.
Why is this company obligated to comply with the GDPR?

A. The company has offices in the EU.
B. The company employs staff in the EU.
C. The company's data center is located in a country outside the EU.
D. The company's products are marketed directly to EU customers.

Correct Answer: D
Section:
Explanation:
You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and Asia. A large portion of the company's revenue is due to international sales.
The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered:

The figures can answer children's Questions: on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well. The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.
When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's question. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.
In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a Near-Field Communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of home and have the character's abilities remain intact.
Why is this company obligated to comply with the GDPR?
A) The company has offices in the EU. B. The company employs staff in the EU. C. The company's data center is located in a country outside the EU. D. The company's products are marketed directly to EU customers.
Answer
Verified Answer:D. The company's products are marketed directly to EU customers.
Comprehensive Explanation:According to section 6(1) of the GDPR1, personal data shall be processed by organisations, which offer goods or services or otherwise carry out activities, in relation to which processing of personal data may be regarded as relevant for their legitimate interests. The legitimate interests referred to are those arising fromthe performanceofa task carried out in their name or on their behalf,orfor their own purposes. The legitimate interests referredto are those arising fromthe performanceofa task carried out in their name or on their behalf,orfor their own purposes. The legitimate interests referredto are those arising fromthe performanceofa task carried out in their name or on their behalf, or for their own purposes. The legitimate interests referredto are those arising fromthe performanceofa task carried out in their name or on their behalf, or for their own purposes. The legitimate interests referredto are those arising fromthe performanceofa task carried out in their name or on their behalf, or for their own purposes. The legitimate interests referredto are those arising fromthe performance

QUESTION 40
With the issue of consent, the GDPR allows member states some choice regarding what?

A. The mechanisms through which consent may be communicated
B. The circumstances in which silence or inactivity may constitute consent
C. The age at which children must be required to obtain parental consent
D. The timeframe in which data subjects are allowed to withdraw their consent

Correct Answer: C
Section:
Explanation:
The GDPR states that the parental consent mechanism generally applies when the child is younger than 16 years1.Processing personal data will be lawful only if the child's parent or custodian has consented to such processing2.However, Member States are allowed to lower this threshold in national legislation up to 13 years old3. This means that Member States have some choice regarding the age limit for children's consent, as long as it is not below 13 years.The GDPR also requires that the consent request is clear and understandable for the child, and that the controller makes reasonable efforts to verify that the consent is given or authorised by the holder of parental responsibility4.Reference:CIPP/E Certification - International Association of Privacy Professionals,Free CIPP/E Study Guide - International Association of Privacy Professionals,GDPR - EUR-Lex,Complying with the GDPR when vulnerable people use smart devices
I hope this helps. If you have any other questions, please let me know. .

QUESTION 41
Which sentence BEST summarizes the concepts of "fairness," "lawfulness" and "transparency'', as expressly required by Article 5 of the GDPR?

A. Fairness and transparency refer to the communication of key information before collecting data; lawfulness refers to compliance with government regulations.
B. 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.
C. Fairness refers to the security of personal data; lawfulness and transparency refers to the analysis of ordinances to ensure they are uniformly enforced.
D. 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.

Correct Answer: A

Section:
Explanation:
According to the UK GDPR, the processing of personal data must be lawful, fair and transparent1.Lawfulness means that there must be a valid legal basis for processing personal data, such as consent, contract, legal obligation, vital interests, public task or legitimate interests1.Fairness means that the processing must not be detrimental, unexpected or misleading to the individuals concerned1.Transparency means that the individuals must be informed about how their data is used, who it is shared with, what rights they have and how they can exercise them1.Therefore, the sentence that best summarizes these concepts is option A, which states that fairness and transparency refer to the communication of key information before collecting data; lawfulness refers to compliance with government regulations.Reference:1 https://ico.org.uk/for-organisations-2/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

QUESTION 42
Article 5(1)(b) of the GDPR states that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." Based on Article 5(1)(b), what is the impact of a member state's interpretation of the word "incompatible''?

A. It dictates the level of security a processor must follow when using and storing personal data for two different purposes.
B. It guides the courts on the severity of the consequences for those who are convicted of the intentional misuse of personal data.
C. It sets the standard for the level of detail a controller must record when documenting the purpose for collecting personal data.
D. It indicates the degree of flexibility a controller has in using personal data in ways that may vary from its original intended purpose.

Correct Answer: D
Section:
Explanation:
The purpose limitation principle requires that personal data be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes. However, the GDPR does not provide a clear definition of what constitutes an incompatible purpose. Instead, it leaves room for interpretation by the member states, taking into account the context and circumstances of the processing. This means that the degree of flexibility a controller has in using personal data for a new purpose may vary depending on the member state's law and guidance. Some factors that may affect the compatibility assessment include the link between the original and the new purpose, the expectations of the data subject, the nature of the data, the impact of the further processing, and the safeguards applied by the controller.Reference:
GDPR Article 5(1)(b), which states the purpose limitation principle.
GDPR Article 6(4), which lists the criteria for assessing the compatibility of a new purpose.
ICO guidance, which explains the purpose limitation principle and provides examples of compatible and incompatible purposes.
[EDPB guidelines], which provide further guidance on the application of the purpose limitation principle.

QUESTION 43
Tanya is the Data Protection Officer for Curtains Inc., a GDPR data controller. She has recommended that the company encrypt all personal data at rest. Which GDPR principle is she following?

A. Accuracy
B. Storage Limitation
C. Integrity and confidentiality
D. Lawfulness, fairness and transparency

Correct Answer: C
Section:
Explanation:
The GDPR requires that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures1.This principle is known as integrity and confidentiality, or sometimes as security2.Encryption is one of the possible technical measures that can be used to protect personal data at rest, as it makes the data unintelligible to anyone who does not have the key to decrypt it3.By recommending that the company encrypts all personal data at rest, Tanya is following the principle of integrity and confidentiality, as she is ensuring that the personal data is secure and protected from unauthorised access or accidental damage.Reference:1: Article 5(1)(f) of the GDPR2:A guide to the data protection principles | ICO3: Encryption | ICO

QUESTION 44
A well-known video production company, based in Spain but specializing in documentaries filmed worldwide, has just finished recording several hours of footage featuring senior citizens in the streets of Madrid. Under what condition would the company NOT be required to obtain the consent of everyone whose image they use for their documentary?

A. If obtaining consent is deemed to involve disproportionate effort.
B. If obtaining consent is deemed voluntary by local legislation.
C. If the company limits the footage to data subjects solely of legal age.
D. If the company's status as a documentary provider allows it to claim legitimate interest.

Correct Answer: D
Section:
Explanation:
According to the GDPR, consent is one of the six lawful bases for processing personal data, but not the only one. The other five are: contract, legal obligation, vital interests, public task and legitimate interests. Legitimate interests can be invoked by controllers who process personal data for their own benefit or for the benefit of third parties, as long as such processing does not override the rights and freedoms of the data subjects, especially if they are children. The GDPR also recognizes that processing personal data for journalistic purposes or the purposes of academic, artistic or literary expression may be necessary for the exercise of the right to freedom of expression and information, which is a legitimate interest. Therefore, the company may not need to obtain the consent of everyone whose image they use for their documentary, if they can demonstrate that their processing is necessary for the purposes of their journalistic, artistic or literary expression, and that they have taken into account the reasonable expectations of the data subjects and the potential impact on their privacy. The company should also comply with any relevant national laws or codes of conduct that may apply to such processing.Reference:
GDPR, Article 6(1)(a)-(f)
GDPR, Recital 47
GDPR, Article 85

QUESTION 45
Which of the following describes a mandatory requirement for a group of undertakings that wants to appoint a single data protection officer?

A. The group of undertakings must obtain approval from a supervisory authority.
B. The group of undertakings must be comprised of organizations of similar sizes and functions.
C. The data protection officer must be located in the country where the data controller has its main establishment.
D. The data protection officer must be easily accessible from each establishment where the undertakings are located.

Correct Answer: D
Section:
Explanation:
According to Article 37(2) of the GDPR, a group of undertakings may appoint a single data protection officer (DPO) provided that the DPO is easily accessible from each establishment12.This means that the DPO should be able to communicate effectively with the data subjects and the supervisory authorities in the relevant languages and jurisdictions, and to perform the tasks referred to in Article 39 of the GDPR34.The accessibility of the DPO does not necessarily depend on the physical location of the DPO, but rather on the availability of the DPO to the relevant stakeholders via various means of communication34. Therefore, the DPO does not have to be located in the country where the data controller has its main establishment, nor does the group of undertakings have to obtain approval from a supervisory authority or be comprised of organizations of similar sizes and functions to appoint a single DPO.Reference:CIPP/E Certification - International Association of Privacy Professionals,Free CIPP/E Study Guide - International Association of Privacy Professionals,GDPR - EUR-Lex,What's different about a group data protection officer?,Data Protection Officers: What US Companies Need to Know - Cooley

QUESTION 46
What obligation does a data controller or processor have after appointing a data protection officer?

A. To ensure that the data protection officer receives sufficient instructions regarding the exercise of his or her defined tasks.
B. To provide resources necessary to carry out the defined tasks of the data protection officer and to maintain his or her expert knowledge.
C. To ensure that the data protection officer acts as the sole point of contact for individuals' Questions: about their personal data.
D. To submit for approval to the data protection officer a code of conduct to govern organizational practices and demonstrate compliance with data protection principles.

Correct Answer: B
Section:
Explanation:

According to the UK GDPR, the controller and the processor must support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge1.The controller and the processor must also ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks and that he or she reports directly to the highest management level of the controller or the processor1.

QUESTION 47
SCENARIO
Please use the following to answer the next question:
Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts.
Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.
Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.
Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.
For what reason would JaphSoft be considered a controller under the GDPR?

A. It determines how long to retain the personal data collected.
B. It has been provided access to personal data in the MarketIQ database.
C. It uses personal data to improve its products and services for its client-base through machine learning.
D. It makes decisions regarding the technical and organizational measures necessary to protect the personal data.

Correct Answer: C
Section:
Explanation:
According to the GDPR, a data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (Art 4(7) of GDPR). A data processor is the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Art 4(8) of GDPR). In this case, JaphSoft would be considered a controller under the GDPR because it uses the personal data it receives from Liem and EcoMick to improve its own products and services through machine learning. This means that JaphSoft determines the purposes and means of this processing activity, which is not covered by the agreement with Liem and EcoMick. JaphSoft also decides how long to retain the personal data, which is another indication of its controller role. The other options are not sufficient to establish JaphSoft as a controller, as they could also apply to a processor. Having access to personal data in the MarketIQ database does not imply that JaphSoft determines the purposes and means of the processing. It could be acting on behalf of Liem and EcoMick, who are the controllers of the data in the database. Making decisions regarding the technical and organizational measures necessary to protect the personal data is also a duty of a processor, who must implement appropriate security measures in accordance with the GDPR and the instructions of the controller (Art 28 and Art 32 of GDPR).Reference:
GDPR, Art 4, Art 28, Art 32
Free CIPP/E Study Guide, p. 15
European Data Protection Law & Practice, p. 123
What is a data controller or a data processor?
CNIL publishes guidance on data processing roles under EU GDPR
Guide for multi-controller situations under the GDPR

QUESTION 48
SCENARIO
Please use the following to answer the next question:
Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which

sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts.
Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.
Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.
Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.
Why would the consent provided by Ms. Iman NOT be considered valid in regard to JaphSoft?

A. She was not told which controller would be processing her personal data.
B. She only viewed the visual representations of the privacy notice Liem provided.
C. She did not read the privacy notice stating that her personal data would be shared.
D. She has never made any purchases from JaphSoft and has no relationship with the company.

Correct Answer: C
Section:
Explanation:
The reason why the consent provided by Ms. Iman would not be considered valid in regard to JaphSoft is not because she did not provide her consent for her personal data to be shared with EcoMick, but because she was not told which controller would be processing her personal data. JaphSoft is a controller, as it determines the purpose and means of the processing of personal data, which is to improve its marketing optimization models and to provide better services to its customers. JaphSoft does not act only on the instructions of Liem and EcoMick, who are the original controllers of the personal data, but rather uses the data for its own benefit and interest. Therefore, JaphSoft should have obtained a separate consent from Ms. Iman, or relied on another lawful basis, such as legitimate interest, to process her personal data. Ms. Iman only gave consent to Liem, not to JaphSoft, and she was not informed that her personal data would be shared with or processed by another controller.

QUESTION 49
SCENARIO
Please use the following to answer the next question:
Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts.
Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.
Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.
Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.
JaphSoft's use of pseudonymization is NOT in compliance with the CDPR because?

A. JaphSoft failed to first anonymize the personal data.

B. JaphSoft pseudonymized all the data instead of deleting what it no longer needed.
C. JaphSoft was in possession of information that could be used to identify data subjects.
D. JaphSoft failed to keep personally identifiable information in a separate database.

Correct Answer: B
Section:
Explanation:
According to the GDPR, pseudonymization is a technique that reduces the linkability of personal data to a specific data subject by replacing identifying attributes with pseudonyms1.Pseudonymization is not a sufficient measure to anonymize personal data, which means that the data cannot be attributed to an identifiable person without additional information2.Pseudonymization can help data controllers and processors to comply with the GDPR principles of data minimization, purpose limitation, and storage limitation, as well as to enhance the security and confidentiality of personal data3.
In this scenario, JaphSoft's use of pseudonymization is not in compliance with the GDPR because of option C: JaphSoft was in possession of information that could be used to identify data subjects.This is because JaphSoft did not keep the additional information (the contact information) separately from the pseudonymized data (the identifying information), and did not apply technical and organizational measures to prevent the re-identification of the data subjects4. This means that JaphSoft could potentially link the personal data to the individuals, and therefore, the data was not effectively pseudonymized. Moreover, JaphSoft did not have a deletion process for the data it received from clients, which could violate the principle of storage limitation that requires personal data to be kept no longer than necessary for the purposes for which they are processed.

QUESTION 50
SCENARIO
Please use the following to answer the next question:
Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts.
Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.
Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.
Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.
Which of the following BEST describes the relationship between Liem, EcoMick and JaphSoft?

A. Liem is a controller and EcoMick is a processor because Liem provides specific instructions regarding how the marketing campaigns should be rolled out.
B. EcoMick and JaphSoft are is a controller and Liem is a processor because EcoMick is sharing its marketing data with Liem for contacts in Europe.
C. JaphSoft is the sole processor because it processes personal data on behalf of its clients.
D. Liem and EcoMick are joint controllers because they carry out joint marketing activities.

Correct Answer: D
Section:
Explanation:
According to the UK GDPR, 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 her''1.One of the requirements for consent to be informed is that the data subject should be aware of the identity of the controller who is processing the personal data2. In this scenario, Ms. Iman only gave consent to Liem to process her personal data for marketing purposes, but she was not informed that JaphSoft, a third-party controller, would also access and process her personal data. Therefore, her consent was not valid in regard to JaphSoft, as she did not know who was processing her personal data and for what purposes.Reference:
UK GDPR Article 4 (11)
UK GDPR Recital 42

QUESTION 51
SCENARIO
Please use the following to answer the next question:
Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts.
Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.
Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.
Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.
Under the GDPR, Liem and EcoMick's contract with MarketIQ must include all of the following provisions EXCEPT?

A. Processing the personal data upon documented instructions regarding data transfers outside of the EEA.
B. Notification regarding third party requests for access to Liem and EcoMick's personal data.
C. Assistance to Liem and EcoMick in their compliance with data protection impact assessments.
D. Returning or deleting personal data after the end of the provision of the services.

Correct Answer: C
Section:

QUESTION 52
When is data sharing agreement MOST likely to be needed?

A. When anonymized data is being shared.
B. When personal data is being shared between commercial organizations acting as joint data controllers.
C. When personal data is being proactively shared by a controller to support a police investigation.
D. When personal data is being shared with a public authority with powers to require the personal data to be disclosed.

Correct Answer: B
Section:
Explanation:
A data sharing agreement is a contract that documents what data is being shared and how it can be used. It can be used to make data sharing lawful and to demonstrate compliance with the accountability principle under the GDPR. A data sharing agreement is most likely to be needed when personal data is being shared between commercial organizations acting as joint data controllers, because they have to determine and agree on their respective roles and responsibilities, such as the purpose and legal basis of the data sharing, the rights of the data subjects, the security measures, and the liability for any breaches. A data sharing agreement is not mandatory, but it is good practice and can help to avoid disputes and confusion. A data sharing agreement may not be needed or may be less detailed in the other scenarios, depending on the circumstances and the nature of the data. For example, anonymized data is not personal data under the GDPR and does not require a data sharing agreement, although it may still be subject to other contractual or ethical obligations. Personal data that is proactively shared by a controller to support a police investigation may be covered by a legal obligation or a public interest, and the controller may not have much control over how the data is used by the police. Personal data that is shared with a public authority with powers to require the personal data to be disclosed may also be subject to a legal obligation or a public interest, and the controller may have to comply with the authority's request without a data sharing agreement.Reference:
Data sharing agreements | ICO, which provides guidance on the benefits and contents of a data sharing agreement.
Data Sharing Agreement - the Definition - GDPR Summary, which explains what a data sharing agreement is and when it can be used.
The role of data sharing and the GDPR | Data Republic, which discusses the impact of the GDPR on data sharing practices.

QUESTION 53
An employee of company ABCD has just noticed a memory stick containing records of client data, including their names, addresses and full contact details has disappeared. The data on the stick is unencrypted and in clear text. It is uncertain what has happened to the stick at this stage, but it likely was lost during the travel of an employee. What should the company do?

A. Notify as soon as possible the data protection supervisory authority that a data breach may have taken place.
B. Launch an investigation and if nothing is found within one month, notify the data protection supervisory authority.
C. Invoke the "disproportionate effort" exception under Article 33 to postpone notifying data subjects until more information can be gathered.
D. Immediately notify all the customers of the company that their information has been accessed by an unauthorized person.

Correct Answer: A
Section:
Explanation:
The GDPR requires that in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons1.A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed2. In this scenario, the company ABCD is the controller of the client data, and the loss of the memory stick containing unencrypted and clear text personal data is a personal data breach that may pose a risk to the rights and freedoms of the data subjects, such as identity theft, fraud, financial loss, or reputational damage.Therefore, the company ABCD should notify the data protection supervisory authority as soon as possible, and provide the information specified in Article 33(3) of the GDPR, such as the nature of the breach, the categories and number of data subjects and personal data records concerned, the likely consequences of the breach, and the measures taken or proposed to address the breach1. Option A is the correct answer, as it reflects the obligation of the controller under the GDPR. Options B, C and D are incorrect, as they do not comply with the GDPR requirements.Option B would delay the notification beyond the 72-hour deadline, which could result in administrative fines or other sanctions3.Option C would misuse the "disproportionate effort" exception, which only applies to the communication of the breach to the data subjects, not to the notification to the supervisory authority, and only when the controller has implemented appropriate technical and organisational protection measures, such as encryption, that render the personal data unintelligible to any person who is not authorised to access it4.Option D would prematurely notify the customers of the company without first notifying the supervisory authority, and without assessing the level of risk and the necessity of such communication, which should be done in consultation with the supervisory authority5.Reference:1: Article 33(1) of the GDPR2: Article 4(12) of the GDPR3: Article 83(4)(a) of the GDPR4: Article 34(3)(a) of the GDPR5: Article 34(1) and (2) of the GDPR

QUESTION 54
Which of the following does NOT have to be included in the records most processors must maintain in relation to their data processing activities?

A. Name and contact details of each controller on behalf of which the processor is acting.
B. Categories of processing carried out on behalf of each controller for which the processor is acting.
C. Details of transfers of personal data to a third country carried out on behalf of each controller for which the processor is acting.
D. Details of any data protection impact assessment conducted in relation to any processing activities carried out by the processor on behalf of each controller for which the processor is acting.

Correct Answer: D
Section:
Explanation:
According to the GDPR, processors must maintain records of all categories of processing activities carried out on behalf of each controller, containing the following information12:
the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
the categories of processing carried out on behalf of each controller;
where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
The records must be in writing, including in electronic form, and must be made available to the supervisory authority on request. The obligation to maintain records does not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.
The GDPR does not require processors to include details of any data protection impact assessment (DPIA) conducted in relation to any processing activities carried out by the processor on behalf of each controller for which the processor is acting. A DPIA is a process to help identify and minimise the data protection risks of a project. It is the responsibility of the controller to carry out a DPIA where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. The processor may assist the controller in carrying out the DPIA, but the processor does not have to document it in its records of processing activities. Therefore, the correct

answer is D.Reference:
GDPR, Article 30(2)
GDPR, Article 35
ICO, Documentation1
ICO, Data protection impact assessments1

QUESTION 55
An unforeseen power outage results in company Z's lack of access to customer data for six hours. According to article 32 of the GDPR, this is considered a breach. Based on the WP 29's February, 2018 guidance, company Z should do which of the following?

A. Notify affected individuals that their data was unavailable for a period of time.
B. Document the loss of availability to demonstrate accountability
C. Notify the supervisory authority about the loss of availability
D. Conduct a thorough audit of all security systems

Correct Answer: B
Section:
Explanation:
According to Article 32 of the GDPR, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing, including the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident1.A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed2. Therefore, a power outage that results in the loss of availability of customer data for six hours is considered a personal data breach under the GDPR.
Based on the WP 29's February, 2018 guidance, which was endorsed by the European Data Protection Board, company Z should document the loss of availability to demonstrate accountability3. The guidance states that controllers must document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken, regardless of whether the breach needs to be notified to the supervisory authority or the data subjects.This documentation must enable the supervisory authority to verify compliance with the GDPR and must be made available to the supervisory authority on request4.
The other options (A, C, and D) are not required by the GDPR or the guidance, although they may be advisable or beneficial depending on the circumstances.Option A is not mandatory, as the GDPR only requires the controller to communicate the personal data breach to the data subject when the breach is likely to result in a high risk to the rights and freedoms of natural persons5. A temporary loss of availability may not pose such a high risk, unless it affects the data subject's essential services or activities.Option C is also not obligatory, as the GDPR only requires the controller to notify the supervisory authority of the personal data breach within 72 hours unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons6. A short-term loss of availability may not entail such a risk, unless it affects a large number of data subjects or sensitive data.
Option D is not specified by the GDPR or the guidance, although it may be a good practice to conduct a thorough audit of all security systems after a personal data breach to identify and address any vulnerabilities or weaknesses that may have contributed to the incident or may lead to future incidents.Reference:
1:Article 32 of the GDPR
2:Article 4 (12) of the GDPR
3:Endorsed WP29 Guidelines
4:Article 33 (5) of the GDPR
5:Article 34 (1) of the GDPR
6:Article 33 (1) of the GDPR
7:Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01
8: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)
9:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

QUESTION 56
In addition to the European Commission, who can adopt standard contractual clauses, assuming that all required conditions are met?

A. Approved data controllers.
B. The Council of the European Union.
C. National data protection authorities.
D. The European Data Protection Supervisor.

Correct Answer: C
Section:
Explanation:
According to Article 46(2) of the GDPR, standard contractual clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) can be used as a legal basis for data transfers to third countries12. This means that, in addition to the European Commission, national data protection authorities can adopt standard contractual clauses, provided that they meet the conditions and requirements set out in the GDPR and obtain the approval of the Commission. The other options are not correct, as approved data controllers, the Council of the European Union and the European Data Protection Supervisor do not have the power to adopt standard contractual clauses under the GDPR.Reference:CIPP/E Certification - International Association of Privacy Professionals,Free CIPP/E Study Guide - International Association of Privacy Professionals,GDPR - EUR-Lex,Standard Contractual Clauses (SCC) - European Commission
I hope this helps. If you have any other questions, please let me know. .

QUESTION 57
SCENARIO
Please use the following to answer the next question:
Zandelay Fashion ('Zandelay') is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland. Martin is their recently appointed data protection officer, who oversees the company's compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.
The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.
In an aggressive bid to build revenue growth, Jerry, the CEO, tells Martin that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company's customers by analyzing their purchases. Martin tells the CEO that: (a) the potential risks of such activities means that Zandelay needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures, Zandelay may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.
Jerry tells Martin that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Zandelay's business plan and associated processing activities.
What would MOST effectively assist Zandelay in conducting their data protection impact assessment?

A. Information about DPIAs found in Articles 38 through 40 of the GDPR.
B. Data breach documentation that data controllers are required to maintain.
C. Existing DPIA guides published by local supervisory authorities.
D. Records of processing activities that data controllers are required to maintain.

Correct Answer: C
Section:
Explanation:
:A data protection impact assessment (DPIA) is a process to help identify and minimise the data protection risks of a project that involves personal data, especially when using new technologies or processing that is likely to result in a high risk to individuals1.The UK GDPR requires data controllers to carry out a DPIA before starting such processing and to consult the supervisory authority if the DPIA indicates a high risk that cannot be mitigated1.The UK GDPR also provides some general guidance on the content and methodology of a DPIA, but it does not prescribe a specific format or procedure1.Therefore, to effectively assist Zandelay in conducting their DPIA, it would be helpful to refer to existing DPIA guides published by local supervisory authorities, such as the ICO in the UK or the DPC in Ireland23.These guides offer more detailed and practical advice on how to conduct a DPIA, what to include in it, how to assess and mitigate the risks, and when to consult the authority23.They also provide templates, checklists, examples, and case studies to illustrate the DPIA process23. By following these guides, Zandelay can ensure that their DPIA is comprehensive, consistent, and compliant with the UK GDPR and the relevant national laws.
The other options are not as effective as option C, because:
Option A: Information about DPIAs found in Articles 38 through 40 of the UK GDPR is too general and vague to assist Zandelay in conducting their DPIA.These articles only outline the basic requirements and principles of a DPIA, but do not provide any specific guidance on how to conduct one, what to include in it, or how to assess and mitigate the risks1. Zandelay would need more detailed and practical advice to effectively perform a DPIA.
Option B: Data breach documentation that data controllers are required to maintain is not relevant to conducting a DPIA.A data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data1.A data controller must document any data breaches, including the facts, effects, and remedial actions taken, and notify the supervisory authority and the affected individuals without undue delay1.However, a data breach is not the same as a data protection risk, which is the potential for adverse effects on individuals as a result of the processing of their personal data2.A DPIA is a proactive and preventive measure to identify and minimise the data protection risks of a project, not a reactive and corrective measure to deal with the consequences of a data breach2.
Option D: Records of processing activities that data controllers are required to maintain are not sufficient to assist Zandelay in conducting their DPIA.A record of processing activities is a document that contains information about the purposes, categories, recipients, transfers, retention periods, and security measures of the processing of personal data by a data controller or a data processor1.A data controller must maintain a record of processing activities under its responsibility and make it available to the supervisory authority upon request1.However, a record of processing activities is not the same as a DPIA, which is a more in-depth and systematic analysis of the data protection risks and the measures to address them2.A record of processing activities may provide some useful information for a DPIA, such as the nature, scope, context, and purposes of the processing,

but it does not cover other aspects, such as the necessity, proportionality, compliance, and impact of the processing2.
https://blog.netwrix.com/2021/02/17/data-protection-impact-assessment/
https://ico.org.uk/for-organisations-2/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

QUESTION 58
SCENARIO
Please use the following to answer the next question:
Zandelay Fashion ('Zandelay') is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland. Martin is their recently appointed data protection officer, who oversees the company's compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.
The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.
In an aggressive bid to build revenue growth, Jerry, the CEO, tells Martin that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company's customers by analyzing their purchases. Martin tells the CEO that: (a) the potential risks of such activities means that Zandelay needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures. Zandelay may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.
Jerry tells Martin that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Zandelay's business plan and associated processing activities.
What must Zandelay provide to the supervisory authority during the prior consultation?

A. An evaluation of the complexity of the intended processing.
B. An explanation of the purposes and means of the intended processing.
C. Records showing that customers have explicitly consented to the intended profiling activities.
D. Certificates that prove Martin's professional qualities and expert knowledge of data protection law.

Correct Answer: B
Section:
Explanation:
According to Article 36 of the GDPR, when a controller intends to process personal data that would result in a high risk to the rights and freedoms of data subjects, and a data protection impact assessment under Article 35 indicates that the risk cannot be mitigated by the controller, the controller must consult the supervisory authority before processing. The purpose of this prior consultation is to seek the advice of the supervisory authority on whether the processing complies with the GDPR and what measures can be taken to ensure compliance. During the prior consultation, the controller must provide the supervisory authority with the following information:
the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
the purposes and means of the intended processing;
the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to the GDPR;
the contact details of the data protection officer, if any;
the data protection impact assessment provided for in Article 35; and
any other information requested by the supervisory authority.
Therefore, the correct answer is B. An explanation of the purposes and means of the intended processing. This information is essential for the supervisory authority to understand the nature and scope of the processing and to assess its compliance with the GDPR. The other options are not required by Article 36, although they may be relevant for other aspects of the GDPR, such as the data protection by design and by default principle (A), the lawfulness of processing , or the designation of the data protection officer (D).Reference:
Article 36 of the GDPR, which regulates the prior consultation with the supervisory authority.
ICO guidance, which explains the process and requirements of the prior consultation.
EDPB guidelines, which provide further guidance on the criteria and procedure of the prior consultation.

QUESTION 59
A company is located in a country NOT considered by the European Union (EU) to have an adequate level of data protection. Which of the following is an obligation of the company if it imports personal data from another organization in the European Economic Area (EEA) under standard contractual clauses?

A. Submit the contract to its own government authority.
B. Ensure that notice is given to and consent is obtained from data subjects.
C. Supply any information requested by a data protection authority (DPA) within 30 days.

D. Ensure that local laws do not impede the company from meeting its contractual obligations.

Correct Answer: D
Section:
Explanation:
The GDPR allows the transfer of personal data to countries outside of the EEA that do not provide an adequate level of data protection, if appropriate safeguards are provided by the data exporter and the data importer1.One of these safeguards are standard contractual clauses (SCCs) adopted by the European Commission, which are model clauses that impose obligations on both parties to ensure that the transfer complies with the GDPR requirements2.The SCCs also include clauses on the rights of the data subjects, the obligations of the data protection authorities, and the liability and indemnification of the parties3.One of the obligations of the data importer under the SCCs is to warrant that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract, and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the SCCs, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract4. Therefore, option D is the correct answer, as it reflects the obligation of the data importer under the SCCs to ensure that local laws do not impede the company from meeting its contractual obligations. Options A, B and C are incorrect, as they are not obligations of the data importer under the SCCs.Option A is not required by the GDPR or the SCCs, as the data importer does not need to submit the contract to its own government authority, unless the law of the country where the data importer is established requires it to do so prior to the transfer or disclosure of personal data5.Option B is not an obligation of the data importer, but of the data exporter, who must provide the data subjects with the information required by Articles 13 and 14 of the GDPR, including the fact that the data will be transferred to a third country and the appropriate safeguards in place6.Option C is not specific to the SCCs, but a general obligation of any controller or processor under the GDPR, who must cooperate with the supervisory authority and make available all information necessary to demonstrate compliance with their obligations7.Reference:1: Article 46(1) of the GDPR2:Standard Contractual Clauses (SCC) - European Commission3:EU Standard Contractual Clauses (Word documents)4: Clause 5(a) of the SCCs for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/6795: Clause 5(b) of the SCCs for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/6796: Clause 9 of the SCCs for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/6797: Article 31 of the GDPR

QUESTION 60
Which of the following countries will continue to enjoy adequacy status under the GDPR, pending any future European Commission decision to the contrary?

A. Greece
B. Norway
C. Australia
D. Switzerland

Correct Answer: D
Section:
Explanation:
Adequacy is a term that the EU uses to describe other countries, territories, sectors or international organisations that it deems to provide an 'essentially equivalent' level of data protection to that which exists within the EU. An adequacy decision is a formal decision made by the EU which recognises that another country, territory, sector or international organisation provides an equivalent level of protection for personal data as the EU does.The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary12.
The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay as providing adequate protection13.On 28 June 2021, the EU Commission published two adequacy decisions in respect of the UK: one for transfers under the EU GDPR; and the other for transfers under the Law Enforcement Directive (LED)2. These decisions contain the European Commission's detailed assessment of the UK's laws and systems for protecting personal data, as well as the legislation designating the UK as adequate.Both adequacy decisions are expected to last until 27 June 20252.
Among the four options given, only Switzerland has been granted an adequacy decision by the EU, which means that it will continue to enjoy adequacy status under the GDPR, pending any future European Commission decision to the contrary. Greece is a member state of the EU, so it does not need an adequacy decision to receive personal data from the EU. Norway is a member of the European Economic Area (EEA), which also includes Iceland and Liechtenstein, and has incorporated the GDPR into its national law, so it also does not need an adequacy decision.Australia has not been recognised as adequate by the EU, so transfers of personal data from the EU to Australia require appropriate safeguards or derogations13. Therefore, the correct answer is D. Switzerland.Reference:
https://pages.iapp.org/Free-Study-Guides_CIPPE-PPC-EU.html https://data-privacy-office.eu/courses/cipp-e-official-training-course/

QUESTION 61
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?

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.

Correct Answer: C
Section:
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 62
Under the GDPR, which of the following is true in regard to adequacy decisions involving cross-border transfers?

A. The European Commission can adopt an adequacy decision for individual companies.
B. The European Commission can adopt, repeal or amend an existing adequacy decision.
C. EU member states are vested with the power to accept or reject a European Commission adequacy decision.
D. To be considered as adequate, third countries must implement the EU General Data Protection Regulation into their national legislation.

Correct Answer: B
Section:
Explanation:
According to Article 45 of the GDPR, the European Commission has the power to determine whether a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection of personal data. This means that personal data can flow from the EU and the EEA to that third country without any further safeguard being necessary. The adequacy decision is based on an assessment of the legal framework, the enforcement mechanisms, the access by public authorities, the international commitments and the cooperation with the EU of the third country or organisation. The European Commission also monitors the functioning of the adequacy decisions and can repeal, amend or suspend them if the level of protection is no longer ensured. The European Commission has so far recognised several countries and organisations as providing adequate protection, such as Japan, Canada, Switzerland, the UK and the EU-US Data Privacy Framework.Reference:GDPR Article 45,Data protection adequacy for non-EU countries,Adequacy decisions | European Data Protection Board

QUESTION 63
Under Article 58 of the GDPR, which of the following describes a power of supervisory authorities in European Union (EU) member states?

A. The ability to enact new laws by executive order.
B. The right to access data for investigative purposes.
C. The discretion to carry out goals of elected officials within the member state.
D. The authority to select penalties when a controller is found guilty in a court of law.

Correct Answer: B
Section:
Explanation:
Article 58 of the GDPR lists the powers of supervisory authorities in EU member states. Among these powers are the investigative powers, which include the right to access data and information from controllers and processors, as well as to access their premises and equipment. This power enables the supervisory authorities to perform their tasks of monitoring and enforcing the GDPR. The other options are not powers of supervisory authorities under Article 58 of the GDPR.Reference:Art. 58 GDPR -- Powers,Article 58 Powers - GDPR,Article 58 GDPR - GDPRhub

QUESTION 64
After leaving the EU under the terms of Brexit, the United Kingdom will seek an adequacy determination. What is the reason for this?

A. The Insurance Commissioner determined that an adequacy determination is required by the Data Protection Act.
B. Adequacy determinations automatically lapse when a Member State leaves the EU.
C. The UK is now a third country because it's no longer subject to the GDPR.
D. The UK is less trustworthy now that its not part of the Union.

Correct Answer: C
Section:
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 EU, regardless of whether the processing takes place in the EU or not.The GDPR 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 EU1.Therefore, after leaving the EU under the terms of Brexit, the UK became a third country for the purposes of the GDPR, meaning that personal data transfers from the EU to the UK are subject to the rules on international data transfers under Chapter V of the GDPR2.In order to ensure the continuity and stability of data flows between the EU and the UK, the UK sought an adequacy decision from the European Commission, which is a formal recognition that a third country provides an equivalent level of data protection to that of the EU3.On 28 June 2021, the European Commission adopted two adequacy decisions in respect of the UK: one for transfers under the GDPR and the other for transfers under the Law Enforcement Directive (LED)4.These decisions allow personal data to flow freely from the EU to the UK without any further safeguard being necessary, and are expected to last until 27 June 2025, unless they are amended, suspended or repealed earlier5.Reference:
GDPR, Article 3
GDPR, Chapter V
Data protection adequacy for non-EU countries, section "Adequacy decisions''
UK government welcomes the European Commission's draft data adequacy decisions
Adequacy, section "What does the EU GDPR adequacy decision say?''

QUESTION 65
To which of the following parties does the territorial scope of the GDPR NOT apply?

A. All member countries of the European Economic Area.
B. All member countries party to the Treaty of Lisbon.
C. All member countries party to the Paris Agreement.
D. All member countries of the European Union.

Correct Answer: C
Section:
Explanation:
The territorial scope of the GDPR is determined by Article 3 of the Regulation, which sets out two main criteria for applying the GDPR to the processing of personal data: the establishment criterion and the targeting criterion. The establishment criterion 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 targeting criterion 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 addition, the GDPR applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.
Therefore, the territorial scope of the GDPR does not depend on the membership of a country to a particular international agreement or organisation, but on the location and activities of the controller or processor and the data subjects involved in the processing. The Paris Agreement is an international treaty on climate change that aims to limit global warming and reduce greenhouse gas emissions. It does not have any direct or indirect relevance to the GDPR or the protection of personal data. Hence, being a party to the Paris Agreement does not affect the applicability of the GDPR to a country or a controller or processor established in that country.
The other options are incorrect because they are either directly or indirectly related to the GDPR or the protection of personal data. The European Economic Area (EEA) consists of all EU member states plus Iceland, Liechtenstein and Norway. The EEA Agreement allows these three countries to participate in the EU's internal market and to adopt most of the EU legislation, including the GDPR. Therefore, the GDPR applies to all EEA countries as if they were EU member states. The Treaty of Lisbon is an international agreement that amends the two treaties which form the constitutional basis of the EU. The Treaty of Lisbon introduces several changes to the EU's institutional structure, decision-making process, and policy areas, including the recognition of the Charter of Fundamental Rights of the EU as legally binding. The Charter of Fundamental Rights of the EU includes the right to the protection of personal data as a fundamental right, and provides the legal basis for the GDPR. Therefore, the GDPR applies to all EU member states that are parties to the Treaty of Lisbon. The European Union (EU) is a political and economic union of 27 member states that are located primarily in Europe. The EU has developed an internal single market through a standardised system of laws that apply in all member states, including the GDPR. Therefore, the GDPR applies to all EU member states by virtue of their membership to the EU.Reference:Art. 3 GDPR -- Territorial scope,Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation,Paris Agreement - Wikipedia,European Economic Area - Wikipedia,Treaty of Lisbon - Wikipedia,European Union - Wikipedia

QUESTION 66
What must a data controller do in order to make personal data pseudonymous?

A. Separately hold any information that would allow linking the data to the data subject.
B. Encrypt the data in order to prevent any unauthorized access or modification.
C. Remove all indirect data identifiers and dispose of them securely.
D. Use the data only in aggregated form for research purposes.

Correct Answer: A
Section:
Explanation:
Pseudonymisation is a method that allows you to switch the original data set (for example, e-mail or a name) with an alias or pseudonym, or, in other words, a value which does not allow the individual to be directly identified1.It is a reversible process that de-identifies data but allows the re-identification later on if necessary1.This is a well-known data management technique highly recommended by the General Data Protection Regulation (GDPR) as one of the data protection methods2.To make personal data pseudonymous, a data controller must separately hold any information that would allow linking the data to the data subject, such as a key or a code, and ensure that this information is kept securely and subject to technical and organisational measures to prevent unauthorised access or re-identification23. The other options are not correct, as they either describe other data protection methods, such as encryption or anonymisation, or do not meet the definition of pseudonymisation under the GDPR.Reference:Pseudonymization according to the GDPR,Pseudonymisation - Wikipedia,Anonymisation and pseudonymisation | Data Protection Commissioner

QUESTION 67
Which of the following entities would most likely be exempt from complying with the GDPR?

A. A South American company that regularly collects European customers' personal data.
B. A company that stores all customer data in Australia and is headquartered in a European Union (EU) member state.
C. A Chinese company that has opened a satellite office in a European Union (EU) member state to service European customers.
D. A North American company servicing customers in South Africa that uses a cloud storage system made by a European company.

Correct Answer: D
Section:
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 EU, regardless of whether the processing takes place in the EU or not (Article 3(1)). The GDPR also applies to the processing of personal data of data subjects who are in the EU by a controller or a 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 (Article 3(2)). Therefore, the GDPR would apply to the following entities:
A South American company that regularly collects European customers' personal data, as it is offering goods or services to data subjects in the EU.
A company that stores all customer data in Australia and is headquartered in a European Union (EU) member state, as it has an establishment in the EU.
A Chinese company that has opened a satellite office in a European Union (EU) member state to service European customers, as it has an establishment in the EU and is offering goods or services to data subjects in the EU.
The GDPR would not apply to the following entity:
A North American company servicing customers in South Africa that uses a cloud storage system made by a European company, as it does not have an establishment in the EU, nor is it offering goods or services to data subjects in the EU, nor is it monitoring their behaviour within the EU. The fact that it uses a cloud storage system made by a European company does not trigger the application of the GDPR, unless the cloud provider is also processing personal data on behalf of the North American company in the context of its activities in the EU.

QUESTION 68
Article 29 Working Party has emphasized that the GDPR forbids "forum shopping'', which occurs when companies do what?

A. Choose the data protection officer that is most sympathetic to their business concerns.
B. Designate their main establishment in member state with the most flexible practices.
C. File appeals of infringement judgments with more than one EU institution simultaneously.
D. Select third-party processors on the basis of cost rather than quality of privacy protection.

Correct Answer: B
Section:
Explanation:
The GDPR aims to harmonize the data protection rules across the EU and to ensure consistent and effective enforcement of those rules. However, the GDPR also recognizes that there may be some differences in the interpretation and application of the law among the member states, depending on their national legislation, culture and practices.Therefore, the GDPR introduces the concept of the "main establishment" of a controller or processor, which is the place where the decisions on the purposes and means of the processing of personal data are taken in the EU1.The main establishment determines which national supervisory authority will act as the lead authority for the cross-border processing activities of that controller or processor, and which national law will apply in case of a dispute or a complaint2.The Article 29 Working Party, which is an advisory body composed of representatives of the national supervisory authorities, the European Data Protection Supervisor and the European Commission, has issued guidelines on how to identify the main establishment of a controller or processor under the GDPR3. The guidelines emphasize that the main establishment must reflect the reality of the processing activities and the effective and real exercise of management power over those activities. The guidelines also warn against the practice of "forum shopping'', which occurs when a controller or processor designates its main establishment in a member state with the most flexible or lenient data protection regime, regardless of the actual location of the decision-making or the data processing. The guidelines state that such a practice is forbidden under the GDPR, and that the supervisory authorities will closely monitor and verify the criteria used by the controllers or processors to determine their main establishment.If the supervisory authorities find that the main establishment does not correspond to the factual situation, they may challenge the designation and apply the relevant corrective measures4.Reference:1Art.4 (16) GDPR -- Definitions - General Data Protection Regulation (GDPR)2Art.56-58 GDPR -- Cooperation and consistency - General Data Protection Regulation (GDPR)3Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - European Data Protection Board4Ibid, p. 14-15.

QUESTION 69
Under Article 9 of the GDPR, which of the following categories of data is NOT expressly prohibited from data processing?

A. Personal data revealing ethnic origin.
B. Personal data revealing genetic data.
C. Personal data revealing financial data.

D. Personal data revealing trade union membership.

Correct Answer: C
Section:
Explanation:
Article 9 of the GDPR prohibits the processing of special categories of personal data, which are data that reveal sensitive information about the data subject and may pose a high risk to their rights and freedoms. The GDPR defines 10 types of personal data as special categories, which are:
personal data revealing racial or ethnic origin;
personal data revealing political opinions;
personal data revealing religious or philosophical beliefs;
personal data revealing trade union membership;
genetic data;
biometric data (where used for identification purposes);
data concerning health;
data concerning a person's sex life; and
data concerning a person's sexual orientation.
Among the answer choices, only option C is not one of these categories, as financial data is not considered to reveal any sensitive information about the data subject. However, financial data is still subject to the general principles and rules of the GDPR, such as lawfulness, fairness, transparency, accuracy, security, etc.Reference:
Special category data | ICO
Art. 9 GDPR Processing of special categories of personal data
Special Categories of Data - International Association of Privacy Professionals

QUESTION 70
When does the GDPR provide more latitude for a company to process data beyond its original collection purpose?

A. When the data has been pseudonymized.
B. When the data is protected by technological safeguards.
C. When the data serves legitimate interest of third parties.
D. When the data subject has failed to use a provided opt-out mechanism.

Correct Answer: C
Section:
Explanation:
Section: (none)
Explanation:
The GDPR provides more latitude for a company to process data beyond its original collection purpose when the data has been pseudonymized, which means that the data can no longer be attributed to a specific data subject without the use of additional information. Pseudonymization is a technique that reduces the linkability of personal data with the data subject, and enhances the security and privacy of the data processing. According to the GDPR, pseudonymization is one of the measures that can help the company to implement the principles of data protection by design and by default, and to demonstrate compliance with the GDPR obligations. Moreover, the GDPR states that the further processing of pseudonymized data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered to be incompatible with the initial purposes, provided that appropriate safeguards are in place to protect the rights and freedoms of the data subjects. Therefore, pseudonymization can enable the company to use the data for other purposes that are beneficial for society or for innovation, without compromising the privacy of the individuals.Reference:
GDPR, Article 4 (5), Article 5 (1) (b), Article 6 (4) (e), Article 25, Article 32 (1) (a), Article 40 (2) (d), Article 89
Free CIPP/E Study Guide, page 17, section 2.4.1
CIPP/E Certification, page 12, section 1.1.3
Cipp-e Study guides, Class notes & Summaries, document "CIPP/E Exam Summary 2023'', page 45, section 2.4.1
[Pseudonymisation techniques and best practices]

QUESTION 71
In which situation would a data controller most likely be able to justify the processing of the data of a child without parental consent?

A. When the data is to be processed for market research.
B. When providing preventive or counselling services to the child.
C. When providing the child with materials purely for educational use.
D. When a legitimate business interest makes obtaining consent impractical.

Correct Answer: B
Section:
Explanation:
Under the GDPR, the processing of personal data of a child on the basis of consent requires the consent of the holder of parental responsibility over the child, unless the child is at least 16 years old or the applicable national law provides for a lower age (not below 13 years). However, there are some situations where the processing of personal data of a child without parental consent may be justified by other lawful grounds, such as the performance of a contract, the compliance with a legal obligation, the protection of vital interests, the performance of a task carried out in the public interest, or the legitimate interests of the controller or a third party. One of these situations is when the processing is necessary for providing preventive or counselling services to the child, especially in the context of information society services. This is recognised by Recital 38 of the GDPR, which states that:
''Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.''
Therefore, the processing of personal data of a child without parental consent may be lawful if it is necessary for providing preventive or counselling services to the child, such as health, education, social or legal services, that are offered directly to the child and that aim to protect the child's well-being, safety, development or rights. This may include, for example, online counselling platforms, sexual health advice services, anti-bullying or mental health support services, or child protection helplines. In such cases, the controller should ensure that the processing is fair, transparent, proportionate and respectful of the child's best interests, and that appropriate safeguards are in place to protect the child's personal data and rights.
The other options are not likely to justify the processing of personal data of a child without parental consent, as they do not meet the criteria of necessity, proportionality or legitimacy. The processing of personal data of a child for market research purposes is not necessary for the performance of a contract, the compliance with a legal obligation, the protection of vital interests, the performance of a task carried out in the public interest, or the legitimate interests of the controller or a third party, and may pose significant risks to the child's privacy and autonomy. Therefore, such processing requires the consent of the holder of parental responsibility over the child, unless the child is old enough to give their own consent. The provision of materials purely for educational use to a child may not require the processing of personal data of the child at all, or may only require the processing of minimal personal data, such as the child's name or email address. In such cases, the processing may be based on the consent of the child, if the child is old enough to understand the implications of their consent, or on the legitimate interests of the controller, if the processing is necessary for the provision of the educational materials and does not override the interests or rights of the child. However, the controller should still inform the child and the holder of parental responsibility about the processing and provide them with the opportunity to object or withdraw their consent. The existence of a legitimate business interest does not automatically justify the processing of personal data of a child without parental consent, as the controller must also consider the impact of the processing on the rights and freedoms of the child, and whether the processing is necessary and proportionate for the pursuit of that interest. Moreover, the controller must balance the legitimate business interest against the interests or rights of the child, and ensure that the processing does not cause any harm or disadvantage to the child. If the processing involves the use of personal data of a child for the purposes of marketing or creating personality or user profiles, the controller must obtain the consent of the holder of parental responsibility over the child, unless the child is old enough to give their own consent, as these purposes pose a high risk to the child's privacy and autonomy.Reference:GDPR Article 6,GDPR Article 8,GDPR Recital 38,Children and the UK GDPR | ICO,Guidelines on consent under Regulation 2016/679 - European Data Protection Board

QUESTION 72
An organisation receives a request multiple times from a data subject seeking to exercise his rights with respect to his own personal data. Under what condition can the organisation charge the data subject for processing the request?

A. Only where the organisation 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 organisation can demonstrate that the request is clearly excessive or misguided.

Correct Answer: D
Section:
Explanation:
1.A request may be manifestly unfounded or excessive if it has no clear purpose, is clearly frivolous or vexatious, is made repeatedly by the same data subject, or goes beyond what is reasonably necessary to fulfil the data subject's request2.In such cases, the organisation can either charge a reasonable fee or refuse to act on the request, but it must be able to justify its decision and inform the data subject of the reasons and their right to lodge a complaint with a supervisory authority or a judicial remedy1. The other options are not correct, as they either do not reflect the conditions for charging a fee under the GDPR, or are not relevant to the

question.Reference:Right of access | ICO,Charge for a Data Subject Request GDPR - GDPR Wiki

QUESTION 73
Which GDPR principle would a Spanish employer most likely depend upon to annually send the personal data of its employees to the national tax authority?

A. The consent of the employees.
B. The legal obligation of the employer.
C. The legitimate interest of the public administration.
D. The protection of the vital interest of the employees.

Correct Answer: B
Section:
Explanation:
According to Article 6 of the GDPR, the processing of personal data is only lawful if and to the extent that at least one of the following applies:
the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
processing is necessary for compliance with a legal obligation to which the controller is subject;
processing is necessary in order to protect the vital interests of the data subject or of another natural person;
processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
In this case, the Spanish employer would most likely depend on the legal obligation of the employer as the lawful basis for sending the personal data of its employees to the national tax authority. This is because the employer is subject to the tax laws and regulations of Spain, which require the employer to report the income and deductions of its employees to the tax authority on an annual basis. The employer must comply with this legal obligation, and the processing of the employees' personal data is necessary for this purpose. The employer does not need to obtain the consent of the employees, as consent is not a valid basis for processing personal data where there is a clear imbalance between the data subject and the controller, such as in the context of employment. The employer also does not need to rely on the legitimate interest of the public administration, as this is not a specific purpose for which the employer is processing the personal data, but rather a general interest that may be served by the tax authority. The employer also does not need to invoke the protection of the vital interest of the employees, as this basis only applies in situations where the processing is necessary to protect someone's life, such as in a medical emergency.Reference:Article 6 GDPR - Lawfulness of processing - General Data Protection Regulation (GDPR),Lawful basis for processing | ICO,Legal obligation as a lawful basis for processing personal data under the GDPR, [Consent in the employment context | ICO], [Vital interests | ICO]

QUESTION 74
An online company's privacy practices vary due to the fact that it offers a wide variety of services. How could it best address the concern that explaining them all would make the policies incomprehensible?

A. Use a layered privacy notice on its website and in its email communications.
B. Identify uses of data in a privacy notice mailed to the data subject.
C. Provide only general information about its processing activities and offer a toll-free number for more information.
D. Place a banner on its website stipulating that visitors agree to its privacy policy and terms of use by visiting the site.

Correct Answer: A
Section:
Explanation:
The GDPR requires that the information provided to data subjects about the processing of their personal data must be concise, transparent, intelligible and easily accessible, using clear and plain language1. However, this can be challenging when the processing activities are complex, diverse or voluminous. Therefore, a good practice is to use a layered privacy notice, which consists of providing a short notice with the key elements of the privacy information, such as the identity of the controller, the purposes and legal basis of the processing, the recipients of the data, the data subject's rights, and the contact details of the data protection officer or the supervisory authority. The short notice can then contain links to more detailed information, either by expanding each section or by directing the user to a separate page or document.This way, the user can easily access the information that is most relevant or important to them, without being overwhelmed by a long and complex notice23.A layered privacy notice can be used on websites, in emails, in mobile apps, or in any other medium where space or attention span is limited4.Reference:1Art.12 GDPR -- Transparent information, communication and modalities for the exercise of the rights of the data subject - General Data Protection Regulation (GDPR)2Layered Notice - International Association of Privacy Professionals3What methods can we use to provide privacy information?| ICO.4Layered Notice - West Virginia.

QUESTION 75

In which of the following cases, cited as an example by a WP29 guidance, would conducting a single data protection impact assessment to address multiple processing operations be allowed?

A. A medical organization that wants to begin genetic testing to support earlier research for which they have performed a DPIA.
B. A data controller who plans to use a new technology product that has already undergone a DPIA by the product's provider.
C. A marketing team that wants to collect mailing addresses of customers for whom they already have email addresses.
D. A railway operator who plans to evaluate the same video surveillance in all the train stations of his company.

Correct Answer: D
Section:
Explanation:
According to the WP29 guidance on DPIA1, conducting a single DPIA to address multiple processing operations is allowed when the following conditions are met:
The processing operations present similar high risks, which would result in very similar mitigating measures;
The DPIA is reviewed and updated regularly to take into account any changes or new risks;
The DPIA is complemented by ad hoc assessments where necessary to address more specific issues.
The WP29 guidance cites the example of a railway operator who plans to evaluate the same video surveillance in all the train stations of his company as a case where a single DPIA would be sufficient, provided that the above conditions are met2. The other options do not meet these conditions, as they involve different types of processing operations, different purposes, different data subjects, or different technologies.Reference:
WP29 guidance on DPIA
WP29 guidance on DPIA, page 16

QUESTION 76
Under Article 30 of the GDPR, controllers are required to keep records of all of the following EXCEPT?

A. Incidents of personal data breaches, whether disclosed or not.
B. Data inventory or data mapping exercises that have been conducted.
C. Categories of recipients to whom the personal data have been disclosed.
D. Retention periods for erasure and deletion of categories of personal data.

Correct Answer: A
Section:
Explanation:
Article 30 of the GDPR requires controllers and processors to maintain records of their processing activities, which include information such as the purposes of the processing, the categories of personal data, the recipients of the data, the retention periods, and the security measures12. However, Article 30 does not require controllers to keep records of incidents of personal data breaches, whether disclosed or not.This is a separate obligation under Article 33 and Article 34, which require controllers to notify the supervisory authority and the data subjects of any personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons34.Reference:1: Article 30 of the GDPR2: What do we need to document under Article 30 of the UK GDPR?| ICO3: Article 33 of the GDPR4: Article 34 of the GDPR
Section: (none)
Explanation:

QUESTION 77
In which scenario is a Controller most likely required to undertake a Data Protection Impact Assessment?

A. When the controller is collecting email addresses from individuals via an online registration form for marketing purposes.
B. When personal data is being collected and combined with other personal data to profile the creditworthiness of individuals.
C. When the controller is required to have a Data Protection Officer.
D. When personal data is being transferred outside of the EEA.

Correct Answer: B
Section:
Explanation:

According to the GDPR, a data protection impact assessment (DPIA) is a process to help identify and minimize the data protection risks of a project. A DPIA is required when the processing is likely to result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of the processing. The GDPR provides a list of examples of processing operations that require a DPIA, such as:
Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences.
Systematic monitoring of a publicly accessible area on a large scale.
Therefore, an example of a scenario where a controller is most likely required to undertake a DPIA is when personal data is being collected and combined with other personal data to profile the creditworthiness of individuals, as this involves a systematic and extensive evaluation of personal aspects based on automated processing and profiling, and may have significant effects on the individuals. The other scenarios are not necessarily indicative of a high risk to the rights and freedoms of natural persons, and do not fall under the examples of processing operations that require a DPIA provided by the GDPR.Reference:Free CIPP/E Study Guide, page 37;CIPP/E Certification, page 18; GDPR, Article 35, Recital 91.
%20the%20General,and%20freedoms%20of%20natural%20persons%27.

QUESTION 78
Which of the following demonstrates compliance with the accountability principle found in Article 5, Section 2 of the GDPR?

A. Anonymizing special categories of data.
B. Conducting regular audits of the data protection program.
C. Getting consent from the data subject for a cross border data transfer.
D. Encrypting data in transit and at rest using strong encryption algorithms.

Correct Answer: B
Section:
Explanation:
The accountability principle found in Article 5, Section 2 of the GDPR requires data controllers to take responsibility for complying with the GDPR and to be able to demonstrate their compliance1.This means that data controllers must implement appropriate technical and organisational measures to ensure and show that they process personal data in accordance with the GDPR2. One of the measures that can demonstrate compliance with the accountability principle is conducting regular audits of the data protection program.Audits are systematic and independent assessments of the data processing activities and the data protection policies and procedures of an organisation3.They can help to identify and address any gaps or risks in the data protection program, as well as to verify the effectiveness and efficiency of the data protection measures3.Audits can also provide evidence of compliance to the supervisory authorities and the data subjects, as well as to enhance the trust and reputation of the organisation3.Therefore, conducting regular audits of the data protection program is a way to demonstrate compliance with the accountability principle.Reference:1: CIPP/E study guide, page 15;Art. 5 GDPR;Accountability principle | ICO2: CIPP/E study guide, page 16;Art. 24 GDPR; [Guide to accountability and governance | ICO]3: CIPP/E study guide, page 91; [Auditing | ICO]; [GDPR Audits: What You Need to Know - IT Governance Blog].

QUESTION 79
SCENARIO
Please use the following to answer the next question:
Dynaroux Fashion ('Dynaroux') is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland. Ronan is their recently appointed data protection officer, who oversees the company's compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.
The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.
In an aggressive bid to build revenue growth, Jonas, the CEO, tells Ronan that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company's customers by analyzing their purchases. Ronan tells the CEO that: (a) the potential risks of such activities means that
Dynaroux needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures, Dynaroux may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.
Jonas tells Ronan that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Dynaroux's business plan and associated processing activities.
Which of the following facts about Dynaroux would trigger a data protection impact assessment under the GDPR?

A. The company will be undertaking processing activities involving sensitive data categories such as financial and children's data.
B. The company employs approximately 650 people and will therefore be carrying out extensive processing activities.
C. The company plans to undertake profiling of its customers through analysis of their purchasing patterns.
D. The company intends to shift their business model to rely more heavily on online shopping.

Correct Answer: C
Section:
Explanation:
According to theFree CIPP/E Study Guide, page 14, "the GDPR requires controllers to carry out a data protection impact assessment (DPIA) prior to processing where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons." The GDPR also provides a list of examples of processing operations that require a DPIA, such as "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person" (Article 35(3)(a)). Therefore, the fact that Dynaroux plans to undertake profiling of its customers through analysis of their purchasing patterns would trigger a DPIA under the GDPR, as it involves a systematic and extensive evaluation of personal aspects based on automated processing that may significantly affect the customers. The other options are not necessarily cases where a DPIA is required, although they may involve other obligations under the GDPR, such as obtaining a valid legal basis, providing adequate safeguards, or informing the data subjects.Reference:
Free CIPP/E Study Guide, page 14
GDPR, Article 35

QUESTION 80
Which mechanism, new to the GDPR, now allows for the possibility of personal data transfers to third countries under Article 42?

A. Approved certifications.
B. Binding corporate rules.
C. Law enforcement requests.
D. Standard contractual clauses.

Correct Answer: A
Section:
Explanation:
According to Article 42 of the GDPR, the Commission may approve certification mechanisms, seals and marks for the purpose of demonstrating the existence of appropriate safeguards for personal data transfers to third countries or international organisations. These certification mechanisms, seals and marks are voluntary and transparent, and are issued by accredited certification bodies or by the competent supervisory authorities. They are subject to the general provisions on certification in Articles 42 and 43 of the GDPR. They are intended to enhance the trust of data subjects and facilitate the free flow of personal data within the Union and beyond. They are also subject to periodic review and withdrawal or suspension if the conditions for certification are not or are no longer met.Reference:
Article 42 of the GDPR
European Data Protection Law & Practice textbook, Chapter 8: Transfers of Personal Data to Third Countries, Section 8.3: Appropriate Safeguards, Subsection 8.3.4: Certification Mechanisms, Seals and Marks
Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation

QUESTION 81
Which sentence best describes proper compliance for an international organization using Binding Corporate Rules (BCRs) as a controller or processor?

A. Employees must sign an ad hoc contractual agreement each time personal data is exported.
B. All employees are subject to the rules in their entirety, regardless of where the work is taking place.
C. All employees must follow the privacy regulations of the jurisdictions where the current scope of their work is established.
D. Employees who control personal data must complete a rigorous certification procedure, as they are exempt from legal enforcement.

Correct Answer: B
Section:
Explanation:
According to Article 47(2)(a) of the GDPR, binding corporate rules (BCRs) must be legally binding and apply to and be enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees1. This means that all employees within the group must comply with the BCRs, irrespective of their location or the jurisdiction where they operate.The other options are incorrect, as they do not reflect the requirements of the GDPR or the guidance of the European Data Protection Board (EDPB) on BCRs23.Reference:
GDPR Article 47(2)(a)
EDPB Guidelines 3/2018 on the territorial scope of the GDPR
EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679

QUESTION 82
With respect to international transfers of personal data, the European Data Protection Board (EDPB) confirmed that derogations may be relied upon under what condition?

A. If the data controller has received preapproval from a Data Protection Authority (DPA), after submitting the appropriate documents.
B. When it has been determined that adequate protection can be performed.
C. Only if the Data Protection Impact Assessment (DPIA) shows low risk.
D. Only as a last resort and when interpreted restrictively.

Correct Answer: D
Section:
Explanation:
The GDPR allows for derogations for specific situations when a transfer of personal data to a third country or an international organization cannot be based on an adequacy decision, appropriate safeguards, or binding corporate rules1. However, these derogations are exceptions to the general rule and should not become the norm.The EDPB confirmed that derogations should only be used as a last resort and when interpreted restrictively, taking into account the nature of the data, the purpose and duration of the processing, the country of origin and destination, and the rights and freedoms of data subjects23.The EDPB also stressed that the data exporter must assess the level of protection in the third country and ensure that the transfer does not undermine the essence of the fundamental rights and freedoms of data subjects23.Reference:1: Article 49 of the GDPR2: Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/6793: A guide to international transfers | ICO

QUESTION 83
SCENARIO
Please use the following to answer the next question:
T-Craze, a German-headquartered specialty t-shirt company, was successfully selling to large German metropolitan cities. However, after a recent merger with another German-based company that was selling to a broader European market, T-Craze revamped its marketing efforts to sell to a wider audience. These efforts included a complete redesign of its logo to reflect the recent merger, and improvements to its website meant to capture more information about visitors through the use of cookies.
T-Craze also opened various office locations throughout Europe to help expand its business. While Germany continued to host T-Craze's headquarters and main product-design office, its French affiliate became responsible for all marketing and sales activities. The French affiliate recently procured the services of Right Target, a renowned marketing firm based in the Philippines, to run its latest marketing campaign. After thorough research, Right Target determined that T-Craze is most successful with customers between the ages of 18 and 22. Thus, its first campaign targeted university students in several European capitals, which yielded nearly 40% new customers for T-Craze in one quarter. Right Target also ran subsequent campaigns for T- Craze, though with much less success.
The last two campaigns included a wider demographic group and resulted in countless unsubscribe requests, including a large number in Spain. In fact, the Spanish data protection authority received a complaint from Sofia, a mid-career investment banker. Sofia was upset after receiving a marketing communication even after unsubscribing from such communications from the Right Target on behalf of T-Craze.
Which of the following is T-Craze's lead supervisory authority?

A. Germany, because that is where T-Craze is headquartered.
B. France, because that is where T-Craze conducts processing of personal information.
C. Spain, because that is T-Craze's primary market based on its marketing campaigns.
D. T-Craze may choose its lead supervisory authority where any of its affiliates are based, because it has presence in several European countries.

Correct Answer: A
Section:
Explanation:
According to the GDPR, the lead supervisory authority is the supervisory authority with the primary responsibility for dealing with a cross-border processing activity, for example when a data subject makes a complaint about the processing of his or her personal data. The lead supervisory authority is determined according to the location of the main establishment or the single establishment of the controller or processor in the EU. The main establishment is the place where the decisions about the purposes and means of the processing are taken, or where the controller has its central administration in the EU. The single establishment is the only place where the controller or processor is established in the EU. Therefore, in this scenario, T-Craze's lead supervisory authority is Germany, because that is where T-Craze is headquartered and where it has its main product-design office, which implies that the decisions about the processing of personal data are taken there. The other options are not correct, because the location of the processing, the market or the affiliates are not relevant for determining the lead supervisory authority.Reference:Free CIPP/E Study Guide, page 39;CIPP/E Certification, page 19; GDPR, Article 4(16), Article 4(22), Article 56, Recital 36.

QUESTION 84
SCENARIO
Please use the following to answer the next question:

T-Craze, a German-headquartered specialty t-shirt company, was successfully selling to large German metropolitan cities. However, after a recent merger with another German-based company that was selling to a broader European market, T-Craze revamped its marketing efforts to sell to a wider audience. These efforts included a complete redesign of its logo to reflect the recent merger, and improvements to its website meant to capture more information about visitors through the use of cookies.
T-Craze also opened various office locations throughout Europe to help expand its business. While Germany continued to host T-Craze's headquarters and main product-design office, its French affiliate became responsible for all marketing and sales activities. The French affiliate recently procured the services of Right Target, a renowned marketing firm based in the Philippines, to run its latest marketing campaign. After thorough research, Right Target determined that T-Craze is most successful with customers between the ages of 18 and 22. Thus, its first campaign targeted university students in several European capitals, which yielded nearly 40% new customers for T-Craze in one quarter. Right Target also ran subsequent campaigns for T- Craze, though with much less success.
The last two campaigns included a wider demographic group and resulted in countless unsubscribe requests, including a large number in Spain. In fact, the Spanish data protection authority received a complaint from Sofia, a mid-career investment banker. Sofia was upset after receiving a marketing communication even after unsubscribing from such communications from the Right Target on behalf of T-Craze.
Why does the Spanish supervisory authority notify the French supervisory authority when it opens an investigation into T-Craze based on Sofia's complaint?

A. T-Craze has a French affiliate.
B. The French affiliate procured the services of Right Target.
C. T-Craze conducts its marketing and sales activities in France.
D. The Spanish supervisory authority is providing a courtesy notification not required under the GDPR.

Correct Answer: C
Section:
Explanation:
According to the CIPP/E study guide, Article 56 of the GDPR establishes the concept of the lead supervisory authority, which is the supervisory authority of the main or single establishment of the data controller or processor in the EU1.The lead supervisory authority has the primary responsibility for dealing with cross-border data processing, in cooperation with other concerned supervisory authorities1.Article 60 of the GDPR requires the lead supervisory authority to cooperate with the other supervisory authorities concerned in an endeavour to reach consensus2.The other supervisory authorities concerned are those that are established in a Member State where the data controller or processor has an establishment or where data subjects are substantially affected or likely to be substantially affected by the processing2. In the scenario, T-Craze is a German-headquartered company that has a French affiliate responsible for all marketing and sales activities. Therefore, the French supervisory authority is the lead supervisory authority for the processing of personal data related to the marketing and sales activities of T-Craze, as it is the supervisory authority of the main establishment of the data controller in the EU. The Spanish supervisory authority is a concerned supervisory authority, as it is the supervisory authority of the Member State where data subjects are likely to be substantially affected by the processing, such as Sofia who filed a complaint.Therefore, the Spanish supervisory authority notifies the French supervisory authority when it opens an investigation into T-Craze based on Sofia's complaint, in order to cooperate with the lead supervisory authority and seek consensus on the action to be taken2.Reference:1: CIPP/E study guide, page 87;Art. 56 GDPR;Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)2: CIPP/E study guide, page 88;Art. 60 GDPR;Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

QUESTION 85
SCENARIO
Please use the following to answer the next question:
T-Craze, a German-headquartered specialty t-shirt company, was successfully selling to large German metropolitan cities. However, after a recent merger with another German-based company that was selling to a broader European market, T-Craze revamped its marketing efforts to sell to a wider audience. These efforts included a complete redesign of its logo to reflect the recent merger, and improvements to its website meant to capture more information about visitors through the use of cookies.
T-Craze also opened various office locations throughout Europe to help expand its business. While Germany
Target, a renowned marketing firm based in the Philippines, to run its latest marketing campaign. After thorough research, Right Target determined that T-Craze is most successful with customers between the ages of 18 and 22. Thus, its first campaign targeted university students in several European capitals, which yielded nearly 40% new customers for T-Craze in one quarter. Right Target also ran subsequent campaigns for T- Craze, though with much less success.
The last two campaigns included a wider demographic group and resulted in countless unsubscribe requests, including a large number in Spain. In fact, the Spanish data protection authority received a complaint from Sofia, a mid-career investment banker. Sofia was upset after receiving a marketing communication even after unsubscribing from such communications from the Right Target on behalf of T-Craze.
What is the best option for the lead regulator when responding to the Spanish supervisory authority's notice that it plans to take action regarding Sofia's complaint?

A. Accept, because it did not receive any complaints.
B. Accept, because GDPR permits non-lead authorities to take action for such complaints.
C. Reject, because Right Target's processing was conducted throughout Europe.
D. Reject, because GDPR does not allow other supervisory authorities to take action if there is a lead authority.

Correct Answer: B

Section:
Explanation:
According to theFree CIPP/E Study Guide, page 16, "the GDPR provides for a one-stop-shop mechanism, which means that a controller or processor with establishments in several Member States will have only one supervisory authority as its interlocutor, which will act as the lead authority. However, this does not mean that the lead authority has exclusive competence to supervise all processing activities of the controller or processor throughout the EU. The GDPR also allows for the possibility of a relevant and reasoned objection by a concerned supervisory authority, which may trigger the consistency mechanism and the involvement of the European Data Protection Board (EDPB). Moreover, the GDPR recognizes the right of any supervisory authority to adopt urgent measures on its own territory or to commence legal proceedings before a court in its Member State in order to protect the rights and freedoms of data subjects." Therefore, the lead regulator should accept the Spanish supervisory authority's notice that it plans to take action regarding Sofia's complaint, as the GDPR permits non-lead authorities to take action for such complaints, especially when they involve urgent measures or legal proceedings to protect the data subjects' rights and freedoms. The other options are incorrect, as they do not reflect the GDPR's provisions on the one-stop-shop mechanism and the cooperation and consistency mechanisms.Reference:
Free CIPP/E Study Guide, page 16
GDPR, Articles 56, 60, 61, 62, 63, 64, 65 and 66

QUESTION 86
Which of the following is one of the supervisory authority's investigative powers?

A. To notify the controller or the processor of an alleged infringement of the GDPR.
B. To require that controllers or processors adopt approved data protection certification mechanisms.
C. To determine whether a controller or processor has the right to a judicial remedy concerning a compensation decision made against them.
D. To require data controllers to provide them with written notification of all new processing activities.

Correct Answer: A
Section:
Explanation:
According to Article 58 of the GDPR, each supervisory authority has the power to notify the controller or the processor of an alleged infringement of the GDPR as part of its investigative powers. This power allows the supervisory authority to alert the controller or the processor of a possible violation of the GDPR and to initiate further actions if necessary. The notification may also include recommendations or instructions on how to remedy the infringement or prevent further violations.Reference:
Article 58 of the GDPR
European Data Protection Law & Practice textbook, Chapter 9: Supervision and Enforcement, Section 9.2: Supervisory Authorities, Subsection 9.2.2: Powers of Supervisory Authorities

QUESTION 87
SCENARIO
Please use the following to answer the next question:
TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.
During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed Questionaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories -- age, income, ethnicity -- that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the Questionaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.
Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.
After Leon has informed his manager, what is Techiva's legal responsibility as a processor?

A. They must report it to TripBliss Inc.
B. They must conduct a full systems audit.

C. They must report it to the supervisory authority.
D. They must inform customers who have used the website.

Correct Answer: A
Section:
Explanation:
:According to Article 33 of the GDPR, processors must notify controllers without undue delay after becoming aware of a personal data breach1.Even though Leon and Fred did not disclose the data to anyone else, the unauthorized access and copying of the log files still constitutes a personal data breach2. Therefore, Techiva, as a processor, has a legal responsibility to report it to TripBliss Inc., as the controller. The other options are not legal obligations for processors, although they may be good practices or contractual terms.Reference:
Free CIPP/E Study Guide, page 32, section 4.1.2
CIPP/E Certification, page 27, section 4.1.2
Cipp-e Study guides, Class notes & Summaries, page 38, section 4.1.2
New IAPP CIPP-E Exam Practice Questions, question 141
Processors' responsibilities, paragraph 2

QUESTION 88
SCENARIO
Please use the following to answer the next question:
Joe is the new privacy manager for Who-R-U, a Canadian business that provides DNA analysis. The company is headquartered in Montreal, and all of its employees are located there. The company offers its services to Canadians only: Its website is in English and French, it accepts only Canadian currency, and it blocks internet traffic from outside of Canada (although this solution doesn't prevent all non-Canadian traffic). It also declines to process orders that request the DNA report to be sent outside of Canada, and returns orders that show a non-Canadian return address.
Bob, the President of Who-R-U, thinks there is a lot of interest for the product in the EU, and the company is exploring a number of plans to expand its customer base.
The first plan, collegially called We-Track-U, will use an app to collect information about its current Canadian customer base. The expansion will allow its Canadian customers to use the app while traveling abroad. He suggests that the company use this app to gather location information. If the plan shows promise, Bob proposes to use push notifications and text messages to encourage existing customers to pre-register for an EU version of the service. Bob calls this work plan, We-Text-U. Once the company has gathered enough pre- registrations, it will develop EU-specific content and services.
Another plan is called Customer for Life. The idea is to offer additional services through the company's app, like storage and sharing of DNA information with other applications and medical providers. The company's contract says that it can keep customer DNA indefinitely, and use it to offer new services and market them to customers. It also says that customers agree not to withdraw direct marketing consent. Paul, the marketing director, suggests that the company should fully exploit these provisions, and that it can work around customers' attempts to withdraw consent because the contract invalidates them.
The final plan is to develop a brand presence in the EU. The company has already begun this process. It is in the process of purchasing the naming rights for a building in Germany, which would come with a few offices that Who-R-U executives can use while traveling internationally. The office doesn't include any technology or infrastructure; rather, it's simply a room with a desk and some chairs.
On a recent trip concerning the naming-rights deal, Bob's laptop is stolen. The laptop held unencrypted DNA reports on 5,000 Who-R-U customers, all of whom are residents of Canad a. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information.
If Who-R-U decides to track locations using its app, what must it do to comply with the GDPR?

A. Get consent from the app users.
B. Provide a transparent notice to users.
C. Anonymize the data and add latency so it avoids disclosing real time locations.
D. Obtain a court order because location data is a special category of personal data.

Correct Answer: A
Section:
Explanation:
According to the GDPR, location data is a type of personal data that can reveal information about an individual's habits, preferences, or movements1.Location data can also be considered as a special category of personal data if it reveals information about an individual's health, ethnic origin, or religious beliefs2.Therefore, location data is subject to the GDPR's rules on the lawful processing of personal data, which require a valid legal basis, such as consent, contract, legal obligation, vital interest, public interest, or legitimate interest2.
In this scenario, Who-R-U decides to track locations using its app, which means that it collects and processes location data from its app users. This data can be used to identify the app users, as well as to infer information about their interests, preferences, or behavior.Therefore, Who-R-U needs to comply with the GDPR, even if it only offers its services to Canadians, because it monitors the behavior of individuals in the EU2.
One of the possible legal bases for processing location data is consent, which means that the app users must give their informed, specific, and freely given agreement to the collection and use of their location data2.Consent must be obtained before the processing starts, and it must be easy to withdraw at any time2.Consent must also be granular, meaning that the app users must be able to choose which purposes and types of location data they

agree to share1.
Therefore, if Who-R-U decides to track locations using its app, it must get consent from the app users, and provide them with clear and transparent information about how, why, and for how long their location data will be processed, who will have access to it, and what rights they have under the GDPR12.Who-R-U must also ensure that the consent is voluntary, and that the app users can opt out of location tracking without affecting the functionality or quality of the app12.Reference:1Policy Brief: Location Data Under Existing Privacy Laws | FPF. Available at:5(Accessed: 11 December 2023)2What is the General Data Protection Regulation (GDPR)? | Cloudflare. Available at:6(Accessed: 11 December 2023).

QUESTION 89
SCENARIO
Please use the following to answer the next question:
Joe is the new privacy manager for Who-R-U, a Canadian business that provides DNA analysis. The company is headquartered in Montreal, and all of its employees are located there. The company offers its services to Canadians only: Its website is in English and French, it accepts only Canadian currency, and it blocks internet traffic from outside of Canada (although this solution doesn't prevent all non-Canadian traffic). It also declines to process orders that request the DNA report to be sent outside of Canada, and returns orders that show a non-Canadian return address.
Bob, the President of Who-R-U, thinks there is a lot of interest for the product in the EU, and the company is exploring a number of plans to expand its customer base.
The first plan, collegially called We-Track-U, will use an app to collect information about its current Canadian customer base. The expansion will allow its Canadian customers to use the app while traveling abroad. He suggests that the company use this app to gather location information. If the plan shows promise, Bob proposes to use push notifications and text messages to encourage existing customers to pre-register for an EU version of the service. Bob calls this work plan, We-Text-U. Once the company has gathered enough pre- registrations, it will develop EU-specific content and services.
Another plan is called Customer for Life. The idea is to offer additional services through the company's app, like storage and sharing of DNA information with other applications and medical providers. The company's contract says that it can keep customer DNA indefinitely, and use it to offer new services and market them to customers. It also says that customers agree not to withdraw direct marketing consent. Paul, the marketing director, suggests that the company should fully exploit these provisions, and that it can work around customers' attempts to withdraw consent because the contract invalidates them.
The final plan is to develop a brand presence in the EU. The company has already begun this process. It is in the process of purchasing the naming rights for a building in Germany, which would come with a few offices that Who-R-U executives can use while traveling internationally. The office doesn't include any technology or infrastructure; rather, it's simply a room with a desk and some chairs.
On a recent trip concerning the naming-rights deal, Bob's laptop is stolen. The laptop held unencrypted DNA reports on 5,000 Who-R-U customers, all of whom are residents of Canad a. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information.
The Customer for Life plan may conflict with which GDPR provision?

A. Article 6, which requires processing to be lawful.
B. Article 7, which requires consent to be as easy to withdraw as it is to give.
C. Article 16, which provides data subjects with a rights to rectification.
D. Article 20, which gives data subjects a right to data portability.

Correct Answer: B
Section:
Explanation:
The Customer for Life plan may conflict with Article 7 of the GDPR, which states that "the data subject shall have the right to withdraw his or her consent at any time" and that "it shall be as easy to withdraw as to give consent''1. The plan violates this principle by stating that customers agree not to withdraw direct marketing consent and that the company can ignore any attempts to do so.This is not a valid way of obtaining or maintaining consent, as consent must be freely given, specific, informed and unambiguous2.Moreover, the plan may also conflict with Article 21 of the GDPR, which gives data subjects the right to object to direct marketing at any time3.Reference:1: Article 7(3) of the GDPR2: Article 4(11) of the GDPR3: Article 21(2) of the GDPR
I hope this helps. If you have any other questions, please feel free to ask.

QUESTION 90
SCENARIO
Please use the following to answer the next question:
Joe is the new privacy manager for Who-R-U, a Canadian business that provides DNA analysis. The company is headquartered in Montreal, and all of its employees are located there. The company offers its services to Canadians only: Its website is in English and French, it accepts only Canadian currency, and it blocks internet traffic from outside of Canada (although this solution doesn't prevent all non-Canadian traffic). It also declines to process orders that request the DNA report to be sent outside of Canada, and returns orders that show a non-Canadian return address.
Bob, the President of Who-R-U, thinks there is a lot of interest for the product in the EU, and the company is exploring a number of plans to expand its customer base.
The first plan, collegially called We-Track-U, will use an app to collect information about its current Canadian customer base. The expansion will allow its Canadian customers to use the app while traveling abroad. He suggests that the company use this app to gather location information. If the plan shows promise, Bob proposes to use push notifications and text messages to encourage existing customers to pre-register for an EU version of the service. Bob calls this work plan, We-Text-U. Once the company has gathered enough pre- registrations, it will develop EU-specific content and services.

Another plan is called Customer for Life. The idea is to offer additional services through the company's app, like storage and sharing of DNA information with other applications and medical providers. The company's contract says that it can keep customer DNA indefinitely, and use it to offer new services and market them to customers. It also says that customers agree not to withdraw direct marketing consent. Paul, the marketing director, suggests that the company should fully exploit these provisions, and that it can work around customers' attempts to withdraw consent because the contract invalidates them.
The final plan is to develop a brand presence in the EU. The company has already begun this process. It is in the process of purchasing the naming rights for a building in Germany, which would come with a few offices that Who-R-U executives can use while traveling internationally. The office doesn't include any technology or infrastructure; rather, it's simply a room with a desk and some chairs.
On a recent trip concerning the naming-rights deal, Bob's laptop is stolen. The laptop held unencrypted DNA reports on 5,000 Who-R-U customers, all of whom are residents of Canada. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information.
If Who-R-U adopts the We-Track-U pilot plan, why is it likely to be subject to the territorial scope of the GDPR?

A. Its plan would be in the context of the establishment of a controller in the Union.
B. It would be offering goods or services to data subjects in the Union.
C. It is engaging in commercial activities conducted in the Union.
D. It is monitoring the behavior of data subjects in the Union.

Correct Answer: D
Section:
Explanation:
According to the GDPR, the territorial scope of the regulation 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 behavior as far as their behavior takes place within the Union1. In this scenario, Who-R-U is not established in the Union, but it is collecting location information of its Canadian customers who use the app while traveling abroad, including in the EU. This constitutes monitoring of their behavior within the Union, and therefore triggers the application of the GDPR.The other options are not correct because: (A) Who-R-U does not have any establishment in the Union, as the naming-rights deal does not involve any technology or infrastructure; (B) Who-R-U is not offering goods or services to data subjects in the Union, as it only targets Canadian customers and blocks internet traffic from outside of Canada; Who-R-U is not engaging in commercial activities conducted in the Union, as it only accepts Canadian currency and does not process orders that request the DNA report to be sent outside of Canada.Reference:1: Article 3(2) of the GDPR;Free CIPP/E Study Guide, page 11.

QUESTION 91
SCENARIO
Please use the following to answer the next question:
Joe is the new privacy manager for Who-R-U, a Canadian business that provides DNA analysis. The company is headquartered in Montreal, and all of its employees are located there. The company offers its services to Canadians only: Its website is in English and French, it accepts only Canadian currency, and it blocks internet traffic from outside of Canada (although this solution doesn't prevent all non-Canadian traffic). It also declines to process orders that request the DNA report to be sent outside of Canada, and returns orders that show a non-Canadian return address.
Bob, the President of Who-R-U, thinks there is a lot of interest for the product in the EU, and the company is exploring a number of plans to expand its customer base.
The first plan, collegially called We-Track-U, will use an app to collect information about its current Canadian customer base. The expansion will allow its Canadian customers to use the app while traveling abroad. He suggests that the company use this app to gather location information. If the plan shows promise, Bob proposes to use push notifications and text messages to encourage existing customers to pre-register for an EU version of the service. Bob calls this work plan, We-Text-U. Once the company has gathered enough pre- registrations, it will develop EU-specific content and services.
Another plan is called Customer for Life. The idea is to offer additional services through the company's app, like storage and sharing of DNA information with other applications and medical providers. The company's contract says that it can keep customer DNA indefinitely, and use it to offer new services and market them to customers. It also says that customers agree not to withdraw direct marketing consent. Paul, the marketing director, suggests that the company should fully exploit these provisions, and that it can work around customers' attempts to withdraw consent because the contract invalidates them.
The final plan is to develop a brand presence in the EU. The company has already begun this process. It is in the process of purchasing the naming rights for a building in Germany, which would come with a few offices that Who-R-U executives can use while traveling internationally. The office doesn't include any technology or infrastructure; rather, it's simply a room with a desk and some chairs.
On a recent trip concerning the naming-rights deal, Bob's laptop is stolen. The laptop held unencrypted DNA reports on 5,000 Who-R-U customers, all of whom are residents of Canada. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information.
Who-R-U is NOT required to notify the local German DPA about the laptop theft because?

A. The company isn't a controller established in the Union.
B. The laptop belonged to a company located in Canada.
C. The data isn't considered personally identifiable financial information.
D. There is no evidence that the thieves have accessed the data on the laptop.

Correct Answer: A
Section:
Explanation:
According to the GDPR, a data breach must be notified to the supervisory authority of the member state where the controller or processor is established, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons1.The GDPR defines a controller as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'2.The GDPR also specifies that a controller or processor is considered to be established in the Union if it has "an effective and real exercise of activity through stable arrangements" in the Union, regardless of its legal form or location of its headquarters3.
In this scenario, Who-R-U is not a controller established in the Union, because it does not have any stable arrangements in the Union that involve the processing of personal data. The company only offers its services to Canadians, and does not target or monitor individuals in the Union. The fact that it has purchased the naming rights for a building in Germany, which comes with a few offices, does not constitute an effective and real exercise of activity in the Union, as the offices do not include any technology or infrastructure for processing personal data, and are only used by executives while traveling internationally. Therefore, Who-R-U is not subject to the GDPR's data breach notification obligation, and is not required to notify the local German DPA about the laptop theft.
Art. 33 GDPR -- Notification of a personal data breach to the supervisory authority
Art. 4 GDPR -- Definitions
Art. 3 GDPR -- Territorial scope
Guidelines 9/2022 on personal data breach notification under GDPR
Guidelines 3/2018 on the territorial scope of the GDPR
I hope this helps you understand the GDPR and data breach notification better. If you have any other questions, please feel free to ask me.

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 data. 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 additional information must Wonderkids provide in their Privacy Statement?

A. How often promotional emails will be sent.
B. Contact information of the hosting company.
C. Technical and organizational measures to protect data.
D. The categories of recipients with whom data will be shared.

Correct Answer: D
Section:
Explanation:
According to Article 13 of the GDPR, when personal data are collected from the data subject, the data controller must provide the data subject with the following information, among others1:
The identity and the contact details of the controller and, where applicable, of the controller's representative;
The contact details of the data protection officer, where applicable;
The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
The recipients or categories of recipients of the personal data, if any;
Where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of

transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
In the scenario, Wonderkids provides some of this information in their Privacy Statement, but not all. They do not specify the categories of recipients with whom they will share the personal data of their customers and their children. They only state that they will share the data with businesses that they see as adding real value to the customers, which is vague and ambiguous. This does not comply with the GDPR requirement to inform the data subjects about the recipients or categories of recipients of their personal data, if any. Therefore, Wonderkids must provide this additional information in their Privacy Statement.
1: Art. 13 GDPR Information to be provided where personal data are collected from the data subject

QUESTION 93
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 data. 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?

A. The requirement to implement technical and organizational measures to protect the data.
B. Controller-to-controller model contract clauses.
C. Audit rights for the data subjects.
D. A non-disclosure agreement.

Correct Answer: A
Section:
Explanation:
The GDPR (General Data Protection Regulation) applies to any organisation that processes personal data of EU residents, regardless of where the processing takes place. Therefore, WonderKids, as a data controller based in France, must comply with the GDPR when it transfers personal data to its hosting service provider in Switzerland, which acts as a data processor on behalf of WonderKids.
According to Article 28 of the GDPR, data controllers must only use data processors that provide sufficient guarantees to implement appropriate technical and organisational measures to ensure the protection of the rights of the data subjects and the security of the data. The data controller and the data processor must also enter into a written contract or other legal act that sets out the subject matter, duration, nature, and purpose of the processing, as well as the obligations and rights of the data controller.
The contract must include, among other things, the following provisions:
The data processor must process the personal data only on documented instructions from the data controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by EU or member state law;
The data processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
The data processor must take all measures required pursuant to Article 32 of the GDPR, which relates to the security of the processing;
The data processor must respect the conditions for engaging another processor, and inform the data controller of any intended changes concerning the addition or replacement of other processors, giving the data controller the opportunity to object to such changes;
The data processor must assist the data controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, which relate to the security of the processing, the notification of personal data breaches, the communication of personal data breaches to data subjects, the data protection impact assessment, and the prior consultation with the supervisory authority;
The data processor must, at the choice of the data controller, delete or return all the personal data to the data controller after the end of the provision of services relating to the processing, and delete existing copies unless EU or member state law requires storage of the personal data;
The data processor must make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including

inspections, conducted by the data controller or another auditor mandated by the data controller.
Therefore, among the four options, the one that must be included in the contract between WonderKids and the hosting service provider is the requirement to implement technical and organisational measures to protect the data, as this is part of the data processor's obligations under Article 28 and Article 32 of the GDPR.
The other options are not mandatory under the GDPR, although they may be advisable or desirable depending on the circumstances. Controller-to-controller model contract clauses are used when personal data is transferred from one data controller to another data controller, not from a data controller to a data processor. Audit rights for the data subjects are not explicitly required by the GDPR, although the data controller must ensure that the data processor allows for and contributes to audits conducted by the data controller or another auditor mandated by the data controller. A non-disclosure agreement may be useful to protect the confidentiality of the personal data, but it is not sufficient to ensure the compliance with the GDPR, as it does not cover all the aspects of the data processing relationship.
GDPR
Web Hosting and GDPR Compliance - What to Look For
The GDPR: Why you need to review your third-party service providers' security
GDPR Compliance for Third-Party Service Providers: Vendor Management

QUESTION 94
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 data. 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 direct marketing information can WonderKids send by email without prior consent of the person booking the childcare?

A. No marketing information at all.
B. Any marketing information at all.
C. Marketing information related to other business operations of WonderKids.
D. Marketing information for products or services similar to those purchased from WonderKids.

Correct Answer: D
Section:
Explanation:
According to the ePrivacy Directive, which regulates direct electronic marketing in the EU, consent is generally required before sending marketing emails or texts.However, there is an exception known as the 'soft opt-in', which allows marketing emails or texts to be sent on an opt-out basis if the recipient's details were collected "in the context of the sale of a product or a service" and the marketing is for "similar products or services" provided by the same organisation12. Therefore, WonderKids can send direct marketing information by email without prior consent of the person booking the childcare, as long as the information is about similar products or services to those purchased from WonderKids, and the person is given a clear and easy way to opt out of receiving such emails. The other options are not allowed under the ePrivacy Directive, unless the person has given explicit consent to receive them.Reference:
Free CIPP/E Study Guide, page 33, section 4.1.3
CIPP/E Certification, page 28, section 4.1.3
Cipp-e Study guides, Class notes & Summaries, page 39, section 4.1.3
Direct marketing rules and exceptions under the GDPR, paragraph 5
Marketing | ICO, section "What does the 'soft opt-in' mean?''

QUESTION 95
An organization conducts body temperature checks as a part of COVID-19 monitoring. Body temperature is measured manually and is not followed by registration, documentation or other processing of an individual's

personal data.
Which of the following best explain why this practice would NOT be subject to the GDPR?

A. Body temperature is not considered personal data.
B. The practice does not involve completion by automated means.
C. Body temperature is considered pseudonymous data.
D. The practice is for the purpose of alleviating extreme risks to public health.

Correct Answer: B
Section:
Explanation:
According to the GDPR, personal data means any information relating to an identified or identifiable natural person1.Body temperature is a type of personal data that can reveal information about an individual's health and therefore constitutes special category data under Article 9 of the GDPR2. However, not every activity involving personal data falls within the scope of the GDPR.The GDPR applies only to the processing of personal data wholly or partly by automated means or 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 system3.
In this scenario, the organization conducts body temperature checks as a part of COVID-19 monitoring. Body temperature is measured manually and is not followed by registration, documentation or other processing of an individual's personal data. This means that the organization does not use any automated means to collect, store, or process the body temperature data, nor does it create or intend to create a filing system that contains such data. Therefore, this practice does not involve any processing of personal data within the meaning of the GDPR and is not subject to its rules and obligations.
The other options are incorrect because:
A)Body temperature is considered personal data, as it can be linked to an identifiable natural person and reveal information about their health2.
C)Body temperature is not considered pseudonymous data, as it is not processed in a way that the data can no longer be attributed to a specific data subject without the use of additional information4.
D)The practice is not for the purpose of alleviating extreme risks to public health, as it is not based on any legal obligation, public interest, or vital interest that would justify the processing of special category data under Article 9 of the GDPR5.

QUESTION 96
When assessing the level of risk created by a data breach, which of the following would NOT have to be taken into consideration?

A. The ease of identification of individuals.
B. The size of any data processor involved.
C. The special characteristics of the data controller.
D. The nature, sensitivity and volume of personal data.

Correct Answer: B
Section:
Explanation:
When assessing the level of risk created by a data breach, the size of any data processor involved would not have to be taken into consideration.According to the GDPR, a data breach is "a 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''1.The GDPR requires data controllers and processors to notify the relevant supervisory authority of a data breach within 72 hours, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons2.The GDPR also requires data controllers to communicate the data breach to the affected data subjects without undue delay, if the breach is likely to result in a high risk to their rights and freedoms3.
The GDPR does not specify the exact criteria for determining the level of risk, but it provides some guidance in Recital 85, which states that "the likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing" . The recital also mentions some factors that could increase the risk, such as the ease of identification of individuals, the special categories of personal data, the large scale of the processing, or the special characteristics of the data controller . Therefore, these factors should be taken into consideration when assessing the level of risk created by a data breach.
However, the size of any data processor involved is not relevant for the risk assessment, as it does not affect the impact of the breach on the data subjects. The data processor is only responsible for processing the personal data on behalf of the data controller, and has no direct relationship with the data subjects . The data processor's obligations in case of a data breach are to notify the data controller without undue delay, and to assist the data controller in complying with its obligations under the GDPR .The data processor's size may affect its ability to fulfill these obligations, but it does not change the level of risk created by the data breach itself.Reference:1: Article 4(12) of the GDPR2: Article 33 of the GDPR3: Article 34 of the GDPR : Recital 85 of the GDPR : Article 4(8) of the GDPR : Article 28 of the GDPR
I hope this helps. If you have any other questions, please feel free to ask.

QUESTION 97

Under Article 80(1) of the GDPR, individuals can elect to be represented by not-for-profit organizations in a privacy group litigation or class action. These organizations are commonly known as?

A. Law firm organizations.
B. Civil society organizations.
C. Human rights organizations.
D. Constitutional rights organizations.

Correct Answer: B
Section:
Explanation:
Article 80(1) of the GDPR states that the data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf1.These not-for-profit bodies, organisations or associations are commonly referred to as civil society organizations, as they represent the interests of citizens and groups in the public sphere2.The other options are not correct because: (A) Law firm organizations are not necessarily not-for-profit or active in the field of data protection; Human rights organizations are a subset of civil society organizations, but not all civil society organizations are focused on human rights; (D) Constitutional rights organizations are also a subset of civil society organizations, but not all civil society organizations are concerned with constitutional rights.Reference:1: Article 80(1) of the GDPR;2:Free CIPP/E Study Guide, page 48.

QUESTION 98
SCENARIO
Please use the following to answer the next question:
BHealthy, a company based in Italy, is ready to launch a new line of natural products, with a focus on sunscreen. The last step prior to product launch is for BHealthy to conduct research to decide how extensively to market its new line of sunscreens across Europe. To do so, BHealthy teamed up with Natural Insight, a company specializing in determining pricing for natural products. BHealthy decided to share its existing customer information -- name, location, and prior purchase history -- with Natural Insight. Natural Insight intends to use this information to train its algorithm to help determine the price point at which BHealthy can sell its new sunscreens.
Prior to sharing its customer list, BHealthy conducted a review of Natural Insight's security practices and concluded that the company has sufficient security measures to protect the contact information. Additionally, BHealthy's data processing contractual terms with Natural Insight require continued implementation of technical and organization measures. Also indicated in the contract are restrictions on use of the data provided by BHealthy for any purpose beyond provision of the services, which include use of the data for continued improvement of Natural Insight's machine learning algorithms.
What is the nature of BHealthy and Natural Insight's relationship?

A. Natural Insight is BHealthy's processor because the companies entered into data processing terms.
B. Natural Insight is BHealthy's processor because BHealthy is sharing its customer information with Natural Insight.
C. Natural Insight is the controller because it determines the security measures to implement to protect data it processes; BHealthy is a co-controller because it engaged Natural Insight to determine pricing for the new sunscreens.
D. Natural Insight is a controller because it is separately determine the purpose of processing when it uses BHealthy's customer information to improve its machine learning algorithms.

Correct Answer: D
Section:
Explanation:
According to the GDPR, a controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data1.A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller1.The controller and the processor must enter into a contract or other legal act that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller2.
In this scenario, BHealthy is the controller for the personal data of its customers, as it determines the purposes and means of the processing, such as conducting research to decide how to market its new line of sunscreens across Europe. Natural Insight is the processor for the personal data that BHealthy shares with it, as it processes the data on behalf of BHealthy for the purpose of determining the price point for the new sunscreens. However, Natural Insight is also a controller for the same personal data when it uses it for its own purpose of improving its machine learning algorithms, which is not part of the contract or legal act with BHealthy.Therefore, Natural Insight is a controller and a processor for the same personal data, depending on the purpose of the processing3.
Art. 4 GDPR -- Definitions
Art. 28 GDPR -- Processor
Guidelines 07/2020 on the concepts of controller and processor in the GDPR
I hope this helps you understand the GDPR and the controller-processor relationship better. If you have any other questions, please feel free to ask me.

QUESTION 99
SCENARIO
Please use the following to answer the next question:
Joe started the Gummy Bear Company in 2000 from his home in Vermont, USA. Today, it is a multi-billion-dollar candy company operating in every continent. All of the company's IT servers are located in Vermont. This year Joe hires his son Ben to join the company and head up Project Big, which is a major marketing strategy to triple gross revenue in just 5 years. Ben graduated with a PhD in computer software from a top university. Ben decided to join his father's company, but is also secretly working on launching a new global online dating website company called Ben Knows Best. Ben is aware that the Gummy Bear Company has millions of customers and believes that many of them might also be interested in finding their perfect match. For Project Big, Ben redesigns the company's online web portal and requires customers in the European Union and elsewhere to provide additional personal information in order to remain a customer. Project Ben begins collecting data about customers' philosophical beliefs, political opinions and marital status. If a customer identifies as single, Ben then copies all of that customer's personal data onto a separate database for Ben Knows Best. Ben believes that he is not doing anything wrong, because he explicitly asks each customer to give their consent by requiring them to check a box before accepting their information. As Project Big is an important project, the company also hires a first year college student named Sam, who is studying computer science to help Ben out. Ben calls out and Sam comes across the Ben Knows Best database. Sam is planning on going to Ireland over Spring Beak with 10 of his friends, so he copies all of the customer information of people that reside in Ireland so that he and his friends can contact people when they are in Ireland. Joe also hires his best friend's daughter, Alice, who just graduated from law school in the U.S., to be the company's new General Counsel. Alice has heard about the GDPR, so she does some research on it. Alice approaches Joe and informs him that she has drafted up Binding Corporate Rules for everyone in the company to follow, as it is important for the company to have in place a legal mechanism to transfer data internally from the company's operations in the European Union to the U.S. Joe believes that Alice is doing a great job, and informs her that she will also be in-charge of handling a major lawsuit that has been brought against the company in federal court in the U.S. To prepare for the lawsuit, Alice instructs the company's IT department to make copies of the computer hard drives from the entire global sales team, including the European Union, and send everything to her so that she can review everyone's information. Alice believes that Joe will be happy that she did the first level review, as it will save the company a lot of money that would otherwise be paid to its outside law firm. Ben's collection of additional data from customers created several potential issues for the company, which would most likely require what?

A. New corporate governance and code of conduct.
B. A data protection impact assessment.
C. A comprehensive data inventory.
D. Hiring a data protection officer.

Correct Answer: A
Section:
Explanation:
Ben's collection of additional data from customers, especially sensitive data such as philosophical beliefs and political opinions, created several potential issues for the company, such as:
The risk of violating the data minimization principle, which requires that personal data collected must be adequate, relevant and limited to what is necessary for the purposes of the processing1.
The risk of infringing the rights and freedoms of the data subjects, who may not be aware of or consent to the secondary use of their data by Ben Knows Best, or the unauthorized access and copying of their data by Sam.
The risk of non-compliance with the GDPR's requirements for processing special categories of data, which include data revealing philosophical beliefs and political opinions.Such data can only be processed under certain conditions, such as explicit consent, substantial public interest, or legal claims2.
The risk of data breaches or losses, as the data is transferred to a separate database, copied by Sam, and stored on the company's servers in Vermont, which may not have adequate security measures or safeguards.
Therefore, the company would most likely require a data protection impact assessment (DPIA) to identify and mitigate these risks.A DPIA is a process that helps assess the impact of the envisaged processing operations on the protection of personal data, and consult with the supervisory authority if the DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk3. The other options are not necessarily required by the GDPR, although they may be good practices or contractual terms.Reference:
Free CIPP/E Study Guide, page 32, section 4.1.2
CIPP/E Certification, page 27, section 4.1.2
The Ultimate CIPP/E Study Guide for 2023, page 36, section 4.1.2
Principles - General Data Protection Regulation (GDPR), Article 5
Special categories of personal data - General Data Protection Regulation (GDPR), Article 9
Data protection impact assessment - General Data Protection Regulation (GDPR), Article 35

QUESTION 100
Which of the following was the first legally binding international instrument in the area of data protection?

A. Convention 108.
B. General Data Protection Regulation.
C. Universal Declaration of Human Rights.

D. EU Directive on Privacy and Electronic Communications.

Correct Answer: A
Section:
Explanation:
Convention 108, also known as the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" was adopted by the Council of Europe in 1981.It was the first legally binding international instrument on data protection and required signatories to take steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data1. The Convention covers both the public and private sectors, and applies to any type of data processing, whether automated or not.The Convention also provides for the establishment of independent supervisory authorities and the facilitation of transborder data flows2.
The other options are incorrect because:
B) The General Data Protection Regulation (GDPR) is a regulation of the European Union that came into force in 2018.It is not the first legally binding international instrument on data protection, but rather a successor of the EU Directive 95/46/EC, which was adopted in 1995 and implemented by the EU member states in their national laws3.
C) The Universal Declaration of Human Rights (UDHR) is a resolution of the United Nations General Assembly that was adopted in 1948. It is not a legally binding international instrument, but rather a declaration of common principles and values that guide the development of human rights law.The UDHR does not explicitly mention data protection, but rather recognizes the right to privacy as a fundamental human right in Article 124.
D) The EU Directive on Privacy and Electronic Communications (e-Privacy Directive) is a directive of the European Union that was adopted in 2002 and amended in 2009.It is not the first legally binding international instrument on data protection, but rather a specific instrument that complements the EU Directive 95/46/EC and the GDPR by providing additional rules for the protection of personal data in the context of electronic communications services5.

QUESTION 101
A multinational company is appointing a mandatory data protection officer. In addition to considering the rules set out in Article 37 (1) of the GDPR, which of the following actions must the company also undertake to ensure compliance in all EU jurisdictions in which it operates?

A. Consult national derogations to evaluate if there are additional cases to be considered in relation to the matter.
B. Conduct a Data Protection Privacy Assessment on the processing operations of the company in all the countries it operates.
C. Assess whether the company has more than 250 employees in each of the EU member-states in which it is established.
D. Revise the data processing activities of the company that affect more than one jurisdiction to evaluate whether they comply with the principles of privacy by design and by default.

Correct Answer: A
Section:
Explanation:
A multinational company that is appointing a mandatory data protection officer (DPO) must also consult national derogations to evaluate if there are additional cases to be considered in relation to the matter.According to Article 37 (1) of the GDPR, a DPO must be designated by the controller or the processor in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences1.However, Article 37 (4) of the GDPR also allows Member States to provide for additional cases where a DPO must be designated by law1. Therefore, a multinational company must consult the national laws of the EU jurisdictions in which it operates to ensure that it complies with any additional requirements for appointing a DPO.
The other options are not correct because they are not directly related to the appointment of a DPO. Conducting a Data Protection Privacy Assessment, assessing the number of employees, and revising the data processing activities are all good practices for ensuring compliance with the GDPR, but they are not mandatory actions for designating a DPO.Moreover, the number of employees is not a relevant criterion for appointing a DPO, as the GDPR does not set any threshold based on the size of the organization2.Reference:1: Article 37 of the GDPR2:Guidelines on Data Protection Officers ('DPOs')

QUESTION 102
The European Parliament jointly exercises legislative and budgetary functions with which of the following?

A. The European Commission.
B. The Article 29 Working Party.
C. The Council of the European Union.
D. The European Data Protection Board.

Correct Answer: C

Section:
Explanation:
According to the Treaty on European Union (TEU), the European Parliament shall, jointly with the Council, exercise legislative and budgetary functions.It shall also exercise functions of political control and consultation as laid down in the Treaties1. The Council of the European Union, also known as the Council, is the institution that represents the governments of the Member States.Together with the European Parliament, it adopts European legislation and coordinates the policies of the Member States2.The other options are not correct because: (A) The European Commission is the institution that proposes and implements EU policies, ensures the application of EU law, and represents the Union in international affairs3; (B) The Article 29 Working Party was an advisory body composed of representatives of the national data protection authorities, the European Data Protection Supervisor and the European Commission.It was replaced by the European Data Protection Board in 20184; (D) The European Data Protection Board is an independent body that ensures the consistent application of the General Data Protection Regulation and promotes cooperation among the national data protection authorities5.Reference:1: Article 14(1) of the TEU;2:The Council of the European Union;3:The European Commission;4:Article 29 Working Party;5: [European Data Protection Board].

QUESTION 103
A U.S. company's website sells widgets. Which of the following factors would NOT in itself subject the company to the GDPR?

A. The widgets are offered in EU and priced in euro.
B. The website is in English and French, and is accessible in France.
C. An affiliate office is located in France but the processing is in the U.S.
D. The website places cookies to monitor the EU website user behavior.

Correct Answer: B
Section:
Explanation:
ccording to 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 Union, regardless of whether the processing takes place in the Union or not1.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.
In this scenario, a U.S. company's website sells widgets to customers in the EU and places cookies to monitor their behavior.These factors would subject the company to the GDPR, as they indicate that the company is offering goods or services and monitoring the behavior of data subjects in the Union2.However, the fact that the website is in English and French, and is accessible in France, would not in itself subject the company to the GDPR, as these factors do not necessarily imply an intention to target customers in the Union3.The language and accessibility of the website are not sufficient to establish a relevant and sufficient degree of stability and continuity of the company's activities in the Union3. Therefore, the correct answer is B.
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?
I hope this helps you understand the GDPR and territorial scope better. If you have any other questions, please feel free to ask me.

QUESTION 104
When does the European Data Protection Board (EDPB) recommend reevaluating whether a transfer tool is effectively providing a level of personal data protection that is in compliance with the European Union (EU) level?

A. After a personal data breach.
B. Every three (3) years.
C. On an ongoing basis.
D. Every year.

Correct Answer: C
Section:
Explanation:
According to the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, exporters of personal data to third countries must monitor, on an ongoing basis, developments in those third countries that could affect the level of protection of the personal data they transfer1. This means that exporters must reevaluate whether the transfer tool they rely on, such as standard contractual clauses, binding corporate rules, codes of conduct, or certification mechanisms, is effectively providing a level of personal data protection that is in compliance with the EU level.The EDPB recommends that exporters document this reevaluation and any changes that result from it1. The EDPB does not specify a fixed time interval for this reevaluation, but rather states that it should be done on an ongoing basis,

taking into account the specific circumstances of each transfer and any relevant developments in the third country.
1: EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, adopted on 18 June 2021, paragraphs 85-86.

QUESTION 105
Which judicial body makes decisions on actions taken by individuals wishing to enforce their rights under EU law?

A. Court of Auditors
B. Court of Justice of European Union
C. European Court of Human Rights
D. European Data Protection Board

Correct Answer: B
Section:
Explanation:
The Court of Justice of the European Union (CJEU) is the judicial body of the EU that makes decisions on issues of EU law and enforces European decisions either in respect to actions taken by the European Commission against a member state or actions taken by individuals to enforce their rights under EU law. The CJEU consists of two courts: the Court of Justice and the General Court. The CJEU ensures the uniform interpretation and application of EU law across the EU and settles disputes between EU institutions, member states, and individuals. The other options are not correct, as they are not the judicial bodies that make decisions on actions taken by individuals wishing to enforce their rights under EU law. The Court of Auditors is the EU's independent external auditor that checks the legality and regularity of the EU's revenue and expenditure, and the soundness of its financial management. The European Court of Human Rights (ECHR) is an international court that oversees the European Convention on Human Rights and Fundamental Freedoms of 1950. The ECHR is not linked to the EU institutions, and it covers human rights laws across Europe, including in many non-EU countries. The European Data Protection Board (EDPB) is an independent body that ensures the consistent application of the GDPR and issues opinions on various aspects of data protection, but it does not have judicial authority.
Court of Justice of the European Union
Court of Justice of the European Union - International Association of Privacy Professionals
Judicial enforcement of EU law | European Foundation for the Improvement of Living and Working Conditions
Competences of the Court of Justice of the European Union

QUESTION 106
SCENARIO
Please use the following to answer the next question:
Sandy recently joined Market4U, an advertising technology company founded in 2016, as their VP of Privacy and Data Governance. Through her first initiative in conducting a data inventory, Sandy learned that Market4U maintains a list of 19 million global contacts that were collected throughout the course of Market4U's existence. Knowing the risk of having such a large amount of data, Sandy wanted to purge all contacts that were entered into Market4U's systems prior to May 2018, unless such contacts had a more recent interaction with Market4U content. However, Dan, the VP of Sales, informed Sandy that all of the contacts provide useful information regarding successful marketing campaigns and trends in industry verticals for Market4U's clients.
Dan also informed Sandy that he had wanted to focus on gaining more customers within the sports and entertainment industry. To assist with this behavior, Market4U's marketing team decided to add several new fields to Market4U's website forms, including forms for downloading white papers, creating accounts to participate in Market4U's forum, and attending events. Such fields include birth date and salary.
What should Sandy give as feedback to Dan and the marketing team regarding the new fields Dan wants to add to Market4U's forms?

A. Make all the fields optional.
B. Only request the information in brackets (i.e., age group and salary range).
C. Eliminate the fields, as they are not proportional to the services being offered.
D. Eliminate the fields as they are not necessary for the purposes of providing white papers or registration for events.

Correct Answer: D
Section:
Explanation:
Sandy should give this feedback to Dan and the marketing team, as it reflects the principle of data minimization, which requires that personal data collected must be adequate, relevant and limited to what is necessary for the purposes of the processing1. Collecting birth date and salary information from customers who want to download white papers or register for events is not necessary for those purposes, and may pose risks for data protection and security.Moreover, such information may fall under the category of special data, which requires explicit consent from the data subjects and can only be processed under certain conditions2. The other options do not comply with the principle of data minimization, as they still involve collecting more data than needed, even if they are optional or in brackets.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
Principles - General Data Protection Regulation (GDPR), Article 5
Special categories of personal data - General Data Protection Regulation (GDPR), Article 9

QUESTION 107
SCENARIO
Please use the following to answer the next question:
Sandy recently joined Market4U, an advertising technology company founded in 2016, as their VP of Privacy and Data Governance. Through her first initiative in conducting a data inventory, Sandy learned that Market4U maintains a list of 19 million global contacts that were collected throughout the course of Market4U's existence. Knowing the risk of having such a large amount of data, Sandy wanted to purge all contacts that were entered into Market4U's systems prior to May 2018, unless such contacts had a more recent interaction with Market4U content. However, Dan, the VP of Sales, informed Sandy that all of the contacts provide useful information regarding successful marketing campaigns and trends in industry verticals for Market4U's clients.
Dan also informed Sandy that he had wanted to focus on gaining more customers within the sports and entertainment industry. To assist with this behavior, Market4U's marketing team decided to add several new fields to Market4U's website forms, including forms for downloading white papers, creating accounts to participate in Market4U's forum, and attending events. Such fields include birth date and salary.
What is the best way that Sandy can gain the insights that Dan seeks while still minimizing risks for Market4U?

A. Conduct analysis only on anonymized personal data.
B. Conduct analysis only on pseudonymized personal data.
C. Delete all data collected prior to May 2018 after conducting the trend analysis.
D. Procure a third party to conduct the analysis and delete the data from Market4U's systems.

Correct Answer: B
Section:
Explanation:
According to the GDPR, pseudonymization is a technique that replaces or removes information in a data set that identifies an individual.Pseudonymized data can no longer be attributed to a specific data subject without the use of additional information, which is kept separately and subject to technical and organizational measures to ensure non-attribution1.Pseudonymization is not a method of anonymization, which means that the data is irreversibly altered in such a way that a data subject can no longer be identified2.Pseudonymized data is still considered personal data and subject to the GDPR, but it benefits from some relaxations of the rules, such as the possibility of further processing for compatible purposes, the exemption from some data subject rights, and the facilitation of data transfers3.
In this scenario, Market4U is an advertising technology company that collects and processes a large amount of personal data from its contacts, including sensitive data such as birth date and salary. This data can be used to gain insights into the preferences and behavior of its potential customers, as well as to identify trends and opportunities in different industry verticals. However, this data also poses significant risks for Market4U, such as data breaches, non-compliance, reputational damage, and legal liability.Therefore, Market4U needs to apply the principle of data minimization, which means that it should only collect and process the data that is necessary and relevant for its purposes, and delete the data that is no longer needed4.
One of the ways that Market4U can achieve data minimization is by pseudonymizing the personal data that it uses for analysis. By doing so, Market4U can reduce the risks associated with the processing of personal data, while still retaining the utility and value of the data for its purposes.Pseudonymization can also help Market4U to comply with other GDPR principles, such as purpose limitation, storage limitation, and integrity and confidentiality5.Pseudonymization can also enable Market4U to rely on legitimate interests as a legal basis for the processing of personal data for analysis, as long as it conducts a balancing test and respects the rights and interests of the data subjects6.
Therefore, the best way that Sandy can gain the insights that Dan seeks while still minimizing risks for Market4U is to conduct analysis only on pseudonymized personal data. This option would allow Market4U to use the data for its legitimate business purposes, without compromising the privacy and security of the data subjects.
The other options are incorrect because:
A) Conducting analysis only on anonymized personal data would not be feasible or effective for Market4U, as anonymization is a very difficult and complex process that requires the removal or alteration of any information that can identify an individual, directly or indirectly. Anonymization may also result in the loss of accuracy, quality, and utility of the data, which would undermine the value and purpose of the analysis.Moreover, anonymization is irreversible, which means that Market4U would not be able to restore the original data if needed2.
C) Deleting all data collected prior to May 2018 after conducting the trend analysis would not be compliant with the GDPR, as it would violate the principle of storage limitation, which requires that personal data should be kept only for as long as necessary for the purposes for which it is processed. Market4U cannot justify the retention of the data for longer than needed, especially if the data is outdated, irrelevant, or excessive.Moreover, deleting the data after the analysis would not eliminate the risks associated with the processing of the data, such as data breaches or unauthorized access4.
D) Procuring a third party to conduct the analysis and delete the data from Market4U's systems would not be a good solution for Market4U, as it would involve the transfer of personal data to another data controller or processor, which would require additional safeguards and obligations under the GDPR. Market4U would still be responsible for ensuring the compliance and security of the data, and would have to enter into a data processing agreement with the third party, as well as inform and obtain the consent of the data subjects, if applicable.Furthermore, procuring a third party would entail additional costs and risks for Market4U, such as losing control and

visibility over the data, or exposing the data to unauthorized or unlawful processing by the third party7.

QUESTION 108
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?

A. If the data protection officer lacks ISO 27001 auditor certification.
B. If the data protection officer is provided by the data processor.
C. If the data protection officer also manages the marketing budget.
D. If the data protection officer receives instructions from the data controller.

Correct Answer: A
Section:
Explanation:
A data controller appointing a data protection officer who lacks ISO 27001 auditor certification would not result in an infringement of Articles 37 to 39 of the GDPR.According to Article 37 (5) of the GDPR, the data protection officer must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 391.However, the GDPR does not specify any formal qualifications or certifications that the data protection officer must have, and leaves it to the discretion of the controller or the processor to determine the level of expertise required, depending on the complexity and sensitivity of the data processing activities2. Therefore, the lack of ISO 27001 auditor certification, which is a standard for information security management systems, does not necessarily mean that the data protection officer is not qualified or competent for the role.
The other options are incorrect because they would result in an infringement of Articles 37 to 39 of the GDPR.According to Article 37 (6) of the GDPR, the data protection officer may be a staff member of the controller or the processor, or fulfil the tasks on the basis of a service contract1.However, the data protection officer must be independent and report directly to the highest management level of the controller or the processor3.Therefore, if the data protection officer is provided by the data processor, there may be a conflict of interest or a lack of autonomy, which would violate Article 38 (3) and (6) of the GDPR4.
According to Article 38 (6) of the GDPR, the data protection officer may fulfil other tasks and duties, provided that they do not result in a conflict of interests4.However, managing the marketing budget would likely involve a conflict of interests, as the data protection officer would have to oversee and advise on the data processing activities related to marketing, which may not be compatible with his or her role as a data protection officer5.Therefore, if the data protection officer also manages the marketing budget, this would infringe Article 38 (6) of the GDPR4.
According to Article 38 (3) of the GDPR, the data protection officer must not receive any instructions regarding the exercise of his or her tasks4.The data protection officer must act in an independent manner and perform the tasks assigned by the GDPR, such as informing and advising the controller or the processor and the employees, monitoring compliance, cooperating with the supervisory authority, and acting as the contact point for data subjects and the supervisory authority6.Therefore, if the data protection officer receives instructions from the data controller, this would infringe Article 38 (3) of the GDPR4.Reference:1: Article 37 of the GDPR2:Guidelines on Data Protection Officers ('DPOs')3: Article 38 (2) of the GDPR4: Article 38 of the GDPR5:Data protection officer (DPO) | European Commission6: Article 39 of the GDPR

QUESTION 109
Data retention in the EU was underpinned by a legal framework established by the Data Retention Directive (2006/24/EC). Why is the Directive no longer part of EU law?

A. The Directive was superseded by the EU Directive on Privacy and Electronic Communications.
B. The Directive was superseded by the General Data Protection Regulation.
C. The Directive was annulled by the Court of Justice of the European Union.
D. The Directive was annulled by the European Court of Human Rights.

Correct Answer: C
Section:
Explanation:
The Data Retention Directive (2006/24/EC) was a legal framework that required Member States to ensure that providers of publicly available electronic communications services or of public communications networks retained certain data for a period of between six months and two years, for the purpose of the prevention, investigation, detection and prosecution of serious crime1.However, on 8 April 2014, the Court of Justice of the European Union (CJEU) declared the Directive invalid, as it entailed a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without limiting the access of the competent national authorities to the data retained to what was strictly necessary2.The CJEU also found that the Directive did not provide sufficient safeguards to ensure effective protection of the data against the risk of abuse and against any unlawful access and use of the data2. Therefore, the Directive is no longer part of EU law.
Directive 2006/24/EC of the European Parliament and of the Council
Court of Justice of the European Union PRESS RELEASE No 54/14
I hope this helps you understand the GDPR and data retention better. If you have any other questions, please feel free to ask me.

QUESTION 110
According to the GDPR, when should the processing of photographs be considered processing of special categories of personal data?

A. When processed with the intent to publish information regarding a natural person on publicly accessible media.
B. When processed with the intent to proceed to scientific or historical research projects.
C. When processed with the intent to uniquely identify or authenticate a natural person.
D. When processed with the intent to comply with a law.

Correct Answer: C
Section:
Explanation:
:According to the GDPR, the processing of photographs should not systematically be considered as processing of special categories of personal data, unless they are covered by the definition of biometric data1.Biometric data is defined as personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification or authentication of that natural person, such as facial images or dactyloscopic data2.Therefore, the processing of photographs is considered processing of special categories of personal data when it involves the use of specific technical means, such as facial recognition, that allow or confirm the unique identification or authentication of a natural person3.Reference:1: Recital 51 of the GDPR2: Article 4(14) of the GDPR3: GDPR, Photographs, and Special Categories of Personal Data.

QUESTION 111
The origin of privacy as a fundamental human right can be found in which document?

A. Universal Declaration of Human Rights 1948.
B. European Convention of Human Rights 1953.
C. OECD Guidelines on the Protection of Privacy 1980.
D. Charier of Fundamental Rights of the European Union 2000.

Correct Answer: A
Section:
Explanation:
The Universal Declaration of Human Rights (UDHR) was adopted by the United Nations General Assembly in 1948 as a response to the atrocities of World War II. It is considered the first global expression of human rights and fundamental freedoms. Article 12 of the UDHR states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." This article is the origin of privacy as a fundamental human right that has influenced many subsequent international and regional instruments, such as the European Convention of Human Rights (ECHR), the OECD Guidelines on the Protection of Privacy, and the Charter of Fundamental Rights of the European Union (CFREU).Reference:
IAPP CIPP/E Study Guide, page 7
[Universal Declaration of Human Rights]
[Article 12 of the UDHR]

QUESTION 112
Which statement provides an accurate description of a directive?

A. A directive speo5es certain results that must be achieved, but each member state is free to decide how to turn it into a national law
B. A directive has binding legal force throughout every member state and enters into force on a set date in all the member states.
C. A directive is a legal act relating to specific cases and directed towards member states, companies 0' private individuals.
D. A directive is a legal act that applies automatically and uniformly to all EU countries as soon as it enters into force.

Correct Answer: A
Section:
Explanation:
According to the EU glossary1, a directive is a legal act that sets out a goal that EU countries must achieve, but leaves them the choice of form and methods to reach it. A directive is binding on the EU countries to which it is

addressed, but it does not apply directly at the national level. Instead, it has to be transposed into national law by the national authorities, usually within a specified time limit. This allows for some flexibility and adaptation to the specific circumstances of each country. A directive is different from a regulation, which is a legal act that applies automatically and uniformly to all EU countries as soon as it enters into force, without needing to be transposed into national law.Reference:
Free CIPP/E Study Guide, page 14, section 2.3
Types of legislation, section 2
What are EU directives?

QUESTION 113
Which of the following regulates the use of electronic communications services within the European Union?

A. Regulator (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015.
B. Regulation (EU) 2017/1953 of the European Parliament and of the Council of 25 October 2017.
C. Directive 2002/58'EC of the European Parliament and of the Council of 12 July 2002.
D. Directive (EU) 2019.789 of the European Parliament and of the Council of 17 April 2019.

Correct Answer: C
Section:
Explanation:
Directive 2002/58/EC, also known as the ePrivacy Directive, regulates the use of electronic communications services within the European Union. It covers issues such as confidentiality of communications, processing of traffic and location data, spam, cookies, and security breaches. It complements and particularises Directive 95/46/EC, also known as the Data Protection Directive, which sets out the general principles for the protection of personal data in the EU. The ePrivacy Directive was amended by Directive 2009/136/EC, which introduced new provisions on consent, cookies, and breach notification. The ePrivacy Directive is currently under review and will be replaced by a new Regulation on Privacy and Electronic Communications (ePrivacy Regulation), which is still being negotiated by the EU institutions.Reference:Directive 2002/58/EC,Directive 2009/136/EC, [ePrivacy Regulation]

QUESTION 114
What was the main failing of Convention 108 that led to the creation of the Data Protection Directive (Directive 95/46/EC)?

A. IT did not account for the rapid growth of the Internet
B. It did not include protections for sensitive personal data
C. It was implemented in a fragmented manner by a small number of states.
D. Its penalties for violations of data protection rights were widely viewed as r sufficient.

Correct Answer: C
Section:
Explanation:
Convention 108 was the first legally binding international instrument in the data protection field, adopted by the Council of Europe in 19811.However, it had some limitations that led to the creation of the Data Protection Directive (Directive 95/46/EC) by the European Union in 19952.One of the main failings of Convention 108 was that it was implemented in a fragmented manner by a small number of states, resulting in divergent and inconsistent national laws and practices3.The Data Protection Directive aimed to harmonize the data protection rules within the EU and to ensure a high level of protection for individuals' rights and freedoms2. Therefore, option C is the correct answer.Option A is incorrect because Convention 108 did account for the rapid growth of the Internet by allowing for amendments and protocols to adapt to technological developments1.Option B is incorrect because Convention 108 did include protections for sensitive personal data, such as those revealing racial origin, political opinions, religious beliefs, health, or sexual life1.Option D is incorrect because Convention 108 did not prescribe specific penalties for violations of data protection rights, but left it to the Parties to adopt appropriate sanctions and remedies1.Reference:
Convention 108 and Protocols
CIPP/E Certification
Convention 108+ and the Data Protection Framework of the EU

QUESTION 115
SCENARIO
Please use the following to answer the next question:
Jane Stan's her new role as a Data Protection Officer (DPO) at a Malta-based company that allows anyone to buy and sell cryptocurrencies via its online platform. The company stores and processes the personal data of its

customers in a dedicated data center located in Malta (EU).
People wishing to trade cryptocurrencies are required to open an online account on the platform. They then must successfully pass a KYC due diligence procedure aimed at preventing money laundering and ensuring compliance with applicable financial regulations.
The non-European customers are also required to waive all their GDPR rights by reading a disclaimer written in bold and belong a checkbox on a separate page in order to get their account approved on the platform.
The customers must likewise accept the terms of service of the platform. The terms of service also include a privacy policy section, saying, among other things, that if a
Are the cybersecurity assessors required to sign a data processing agreement with the company in order to comply with the GDPR''

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

Correct Answer: D
Section:
Explanation:
According to the GDPR, a data processor is any person or entity that processes personal data on behalf of a data controller1.A data controller is the one who determines the purposes and means of the processing of personal data1.A data processing agreement (DPA) is a contractual document that sets out the rights and obligations of both parties regarding data protection2.The GDPR requires that a data controller who engages a data processor must enter into a written contract or legal act along the lines set out in Article 28.3 of the GDPR3.The DPA must specify, among other things, the subject matter, duration, nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller3.
In this scenario, the company is the data controller, as it determines the purposes and means of processing the personal data of its customers. The cybersecurity assessors are data processors, as they process the personal data of the customers on behalf of the company. The assessors have access to the personal data, even if it is encrypted, and they perform a specific technical service for the company. Therefore, the assessors are required to sign a DPA with the company in order to comply with the GDPR.The DPA will define the scope, nature and purpose of the processing, the security measures to be implemented, the notification procedures in case of a data breach, and the rights and obligations of both parties.Reference:1: Article 4 of the GDPR2: Data Processing Agreement (Template) - GDPR.eu3: Article 28 of the GDPR.

QUESTION 116
SCENARIO
Please use the following to answer the next question:
Jane Stan's her new role as a Data Protection Officer (DPO) at a Malta-based company that allows anyone to buy and sell cryptocurrencies via its online platform. The company stores and processes the personal data of its customers in a dedicated data center located in Malta |EU).
People wishing to trade cryptocurrencies are required to open an online account on the platform. They then must successfully pass a KYC due diligence procedure aimed at preventing money laundering and ensuring compliance with applicable financial regulations.
The non-European customers are also required to waive all their GDPR rights by reading a disclaimer written in bold and belong a checkbox on a separate page in order to get their account approved on the platform.
The customers must likewise accept the terms of service of the platform. The terms of service also include a privacy policy section, saying, among other things, that if a
Which of the following must be a component of the anti-money-laundering data-sharing practice of the platform?

A. The terms of service shall also enumerate all applicable anti-money laundering few.
B. Customers shall have an opt-out feature to restrict data sharing with law enforcement agencies after the registration.
C. The terms of service shall include the address of the anti-money laundering agency and contacts of the investigators who may access me data.
D. Customers snail receive a clear and conspicuous notice about such data sharing before submitting their data during the registration process.

Correct Answer: D
Section:
Explanation:
According to Article 13 of the GDPR, when personal data are collected from the data subject, the controller shall provide the data subject with certain information, such as the purposes and legal basis of the processing, the recipients or categories of recipients of the personal data, and the existence of the data subject's rights. This information shall be provided at the time when personal data are obtained. The purpose of this requirement is to ensure that the data subject is informed and aware of how their personal data will be used and shared, and to enable them to exercise their rights accordingly. Therefore, customers shall receive a clear and conspicuous notice about such data sharing before submitting their data during the registration process.Reference:
Article 13 of the GDPR
IAPP CIPP/E Study Guide, page 32

QUESTION 117
SCENARIO
Please use the following to answer the next question:
Jane Stan's her new role as a Data Protection Officer (DPO) at a Malta-based company that allows anyone to buy and sell cryptocurrencies via its online platform. The company stores and processes the personal data of its customers in a dedicated data center located m Malta |EU).
People wishing to trade cryptocurrencies are required to open an online account on the platform. They then must successfully pass a KYC due diligence procedure aimed at preventing money laundering and ensuring compliance with applicable financial regulations.
The non-European customers are also required to waive all their GDPR rights by reading a disclaimer written in bold and belong a checkbox on a separate page in order to get their account approved on the platform.
The customers must likewise accept the terms of service of the platform. The terms of service also include a privacy policy section, saying, among other things, that if a
What is potentially wrong with the backup system operated in the AWS cloud?

A. The AWS servers are located in the EU but in a country different than the location of the corporate headquarters.
B. It is unlawful to process any personal data in a cloud unless the cloud is certified as GOPR-compliant by a competent supervisory authority.
C. The data storage period has to be revised, and a data processing agreement w*h AWS must be signed
D. AWS is a U S company, and no personal data of European residents may be transferred to it without explicit written consent from data subjects.

Correct Answer: C
Section:
Explanation:
According to the GDPR, personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed1. Therefore, the data storage period of the backup system must be aligned with this principle and reviewed regularly.Moreover, the GDPR requires that when a controller (the company) uses a processor (AWS) to process personal data on its behalf, it must ensure that the processor provides sufficient guarantees to implement appropriate technical and organizational measures to meet the requirements of the GDPR and ensure the protection of the rights of the data subjects2.This is usually done by signing a data processing agreement that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller3.AWS offers a GDPR-compliant Data Processing Addendum (DPA) that is incorporated into the AWS Service Terms and applies automatically to all customers who require it to comply with the GDPR4.Reference:
Free CIPP/E Study Guide, page 24, section 4.2.1
Free CIPP/E Study Guide, page 25, section 4.3
GDPR, Article 28
GDPR - Amazon Web Services (AWS), section "GDPR resources''

QUESTION 118
A dynamic Internet Protocol (IP) address is considered persona! data when it is combined with what?

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).

Correct Answer: B
Section:
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

QUESTION 119

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?

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

Correct Answer: A
Section:
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 120
Which of the following is NOT exempt from the material scope of the GDPR. insofar as the processing of personal data is concerned?

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.

Correct Answer: A
Section:
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 121
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 data.
Is MagicClean subject to the GDPR?

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.

Correct Answer: D
Section:
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 122
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?

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.

Correct Answer: A
Section:
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 123
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?

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

Correct Answer: A
Section:

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 124
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?

A. Privacy dashboard notice
B. Visualization notice.
C. Just-in-lime notice.
D. Layered notice.

Correct Answer: A
Section:
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?