Free Questions for PDP9 by certscare

Shared by Maldonado on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company based in France uses a specialist IT support business in China The two companies have signed a Data Processing Agreement. The Chinese business provides specialist IT support for the French company's digital customer experience platform No personal data is sent to China, but employees of the Chinese business access the platform on a regular basis and have access to the databases that sit behind it. Which of the following statements is CORRECT in relation to the French company's requirements to ensure compliance with the GDPR?

Options:

A- No personal data is being transferred, therefore no transfer mechanism is needed

B- The French company must identify and implement an appropriate transfer mechanism

C- There is a Data Processing Agreement in place therefore no transfer mechanism is needed

D- China provides an adequate level of protection for personal data, therefore no transfer mechanism is needed

Answer:

B

Explanation:

According to the GDPR, a transfer of personal data to a third country or an international organisation occurs when the personal data is made available to someone outside the EU and EEA, regardless of whether the data is physically sent or not. Therefore, the fact that the Chinese business accesses the platform and the databases that contain personal data of the French company's customers constitutes a transfer of personal data to China, which is a third country under the GDPR. The French company, as the controller of the personal data, must ensure that the transfer complies with the GDPR requirements and that the level of protection of the personal data is not undermined. This means that the French company must identify and implement an appropriate transfer mechanism, such as an adequacy decision, appropriate safeguards, or derogations for specific situations, as set out in Chapter V of the GDPR. A data processing agreement, although necessary to define the roles and responsibilities of the controller and the processor, is not sufficient to ensure the legality of the transfer, as it does not provide the same guarantees as the GDPR. China is not a country that has been recognised by the European Commission as providing an adequate level of protection for personal data, so the French company cannot rely on an adequacy decision either.Reference:

Article 44 of the GDPR1

ICO guidance on international transfers2

Question 2

Question Type: **MultipleChoice**

Where a processor engages another processor ("sub-processor") to carry out processing activities on behalf of a controller, which of the following statements is CORRECT?

Options:

A- The processor must receive prior written authorisation to use the sub-processor

B- The processor may use the sub-processor without the written authorisation of the controller if it adheres to an approved code of conduct

C- The processor may use the sub-processor without the written authorisation of the controller if the sub-processor signs a contract which reflects the same obligations as the contract with the controller

D- The processor may use the sub-processor without the written authorisation of the controller if the processing is deemed to be low risk.

Answer:

A

Explanation:

Article 28(2) of UK GDPR states that where a processor engages another processor ("sub-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 domestic law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of UK GDPR. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall 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. The other options are incorrect, as they do not reflect the requirements of UK GDPR for using a sub-processor. The

processor cannot use a sub-processor without the written authorisation of the controller, regardless of whether it adheres to an approved code of conduct, signs a contract with the same obligations as the controller, or deems the processing to be low risk.Reference:

Article 28(2) of UK GDPR1

ICO guidance on contracts and liabilities between controllers and processors3

Question 3

Question Type: **MultipleChoice**

Describe the act of processing under the authority of a controller or processor as stipulated in UK GDPR Article 29.

Options:

A- The processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

B- A processor shall not process those data except on instructions from the controller, unless required to do so by domestic law

C- Each processor and, where applicable, the processors representative shall maintain a record of all categories of processing activities earned out on behalf of a controller.

D- The processor shall consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the processor to mitigate the risk.

Answer:

B

Explanation:

Article 29 of UK GDPR states that the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by domestic law. This means that the processor must follow the controller's directions on how to handle the personal data, and cannot use it for its own purposes or deviate from the agreed terms. The only exception is when the processor is obliged by law to process the data in a different way, for example, to comply with a court order or a legal obligation. The other options are not related to Article 29, but to other articles of UK GDPR, such as Article 25 (data protection by design and by default), Article 30 (records of processing activities), and Article 36 (prior consultation).Reference:

Article 29 of UK GDPR1

ICO guidance on controllers and processors2

Question 4

Question Type: MultipleChoice

Two businesses decide to work together to sell their products by mail order Orders are made via a single online website and they each use their existing employees to administer and update each other's orders on a single order system regardless of product.

Which of the below is CORRECT of the roles of the two businesses in relation to the single order system'?

Options:

A- They are controllers of their own information contained in the single order system only

B- They are controllers of their own information in the single order system and processors of the information they process on behalf of the other business.

C- The businesses are controllers of their respective information, and the staff are processors of this information

D- They are both joint controllers of the information contained in the single order system

Answer:

D

Explanation:

The two businesses are both joint controllers of the information contained in the single order system, because they jointly determine the purposes and means of the processing. They have a shared purpose of selling their products by mail order and they agree on the means of processing by using a single online website and a single order system. Their decisions complement each other and are necessary for the processing to take place. The processing by each party is inseparable and inextricably linked. Therefore, they meet the criteria for joint controllership under the GDPR.Reference:

Article 26 of the GDPR1

Guidelines 07/2020 on the concepts of controller and processor in the GDPR2, pp. 16-24

Question 5

Question Type: **MultipleChoice**

Which of the following is NOT a processor obligation?

Options:

A- To follow the instructions of the controller in processing personal data

B- To consult the controller prior to appointing any processor.

C- To provide the controller with corporate information relating to its board members.

D- To inform the controller of any intended changes of other processors so they can object

Answer:

C

Explanation:

Providing the controller with corporate information relating to its board members is not a processor obligation under the GDPR. The processor obligations under the GDPR are mainly the following:

To process the personal data only on documented instructions from the controller, unless required by law;

To ensure that persons authorised to process the personal data are bound by confidentiality;

To implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk;

To not engage another processor without the prior authorisation of the controller;

To assist the controller in fulfilling its obligations regarding data subject rights, data protection impact assessments, prior consultations, and data breach notifications;

To delete or return the personal data to the controller at the end of the service, unless required by law to store the data;

To make available to the controller all information necessary to demonstrate compliance and allow for audits and inspections.Reference:

Article 28 of the GDPR1

Guidelines 07/2020 on the concepts of controller and processor in the GDPR2, pp. 37-41

Question 6

Question Type: MultipleChoice

What factors should be considered when looking at security of processing under Article 32 of the GDPR?

Select the INCORRECT answer

Options:

A- Lawfulness of processing

B- The most secure option available

C- The likelihood of a risk to the rights of the data subjects

D- Adherence to an approved code of conduct

Answer:

A

Explanation:

Lawfulness of processing is not a factor that should be considered when looking at security of processing under Article 32 of the GDPR. Lawfulness of processing is a separate requirement that applies to all processing of personal data, regardless of the level of security. Security of processing under Article 32 of the GDPR should be based on the following factors:

The state of the art and the costs of implementation of the security measures;

The nature, scope, context and purposes of the processing;

The risk of varying likelihood and severity for the rights and freedoms of natural persons;

Adherence to an approved code of conduct or an approved certification mechanism (as an element to demonstrate compliance).Reference:

Article 32 of the GDPR1

Guidelines 07/2020 on the concepts of controller and processor in the GDPR2, p. 36

Question 7

Question Type: MultipleChoice

A privacy notice MUST NOT contain

Options:

A- The contact details of the controller

B- The purpose of the processing

C- Details of the processor's staff

D- Details of the right to lodge a complaint with the supervisory authority

Answer:

C

Explanation:

A privacy notice is a document that provides individuals with information about how their personal data is processed, as required by Article 13 and 14 of the UK GDPR5. A privacy notice must include the following information, among others:

the identity and contact details of the controller and, where applicable, the controller's representative and the data protection officer;

the purposes and legal basis of the processing;

the categories of personal data concerned;

the recipients or categories of recipients of the personal data, including any third parties or international organisations;

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 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;

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

the existence of the rights of the data subject, such as the right to access, rectify, erase, restrict, object or port the data, and the conditions or limitations on those rights;

the existence of the right to withdraw consent at any time, where the processing is based on consent;

the right to lodge a complaint with a supervisory authority;

whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

A privacy notice does not need to contain details of the processor's staff, as this is not relevant or necessary for the data subject to understand how their personal data is processed. However, the controller may need to inform the data subject if their personal data is shared with a processor, and provide the identity and contact details of the processor, as part of the information on the recipients or categories of recipients of the personal data.Reference:

Article 13 and 14 of the UK GDPR5

Question 8

Question Type: MultipleChoice

Which of the following statements are CORRECT about records of processing'?

A, It must contain contact details for the Data Protection Officer where applicable.

B, It must be submitted to the Information Commissioner's Office following every Data Protection Impact Assessment

C, It is mandatory for all data processors

D, The controller or the processor a must makes the record available to the supervisory authority on request

E, It must contain contact details for the supervisory authority

Options:

A- B, C. and D

B- A, C, and E

C- A. C, D, and E

D- A, C, and D

Answer:

D

Explanation:

Article 30 of the UK GDPR3requires both controllers and processors to maintain records of their processing activities, unless they are exempted under certain conditions. The records must contain the following information, among others:

the name and contact details of the controller or the processor, and of any joint controller, representative or data protection officer;

the purposes of the processing;

the categories of data subjects and personal data;

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

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 the documentation of suitable safeguards;

where possible, the envisaged time limits for erasure of the different categories of data;

where possible, a general description of the technical and organisational security measures.

The records must be in writing, including in electronic form, and must be made available to the ICO on request. The records do not need to contain contact details of the supervisory authority, as this is not specified in Article 30. Nor do they need to be submitted to the ICO following every DPIA, as this is not required by Article 35, which only obliges the controller to consult the ICO prior to the processing 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.Reference:

Article 30 of the UK GDPR3

Article 35 of the UK GDPR4

Question 9

Question Type: **MultipleChoice**

You are a consulting Data Protection Officer (DPO) for a holiday resort You have been asked to conduct a Data Protection Impact Assessment (DPIA) for them in advance of adopting a new HR management database.

While working through the DPIA, which of the following is NOT a requirement?

Options:

A- Describe the processing

B- Sign off and record outcomes.

C- Identify measures to mitigate the risks

D- Publish any potential risks in your information notice.

Answer:

D

Explanation:

A DPIA is a process to help identify and minimise the data protection risks of a project that is likely to result in a high risk to individuals.A DPIA must include the following elements, according to Article 35(7) of the UK GDPR1:

a description of the processing, including its purposes and legal basis;

an assessment of the necessity and proportionality of the processing in relation to its purposes;

an assessment of the risks to the rights and freedoms of individuals; and

the measures envisaged to address the risks and demonstrate compliance with the UK GDPR.

There is no requirement to publish any potential risks in the information notice, which is a document that provides individuals with information about how their personal data is processed, as required by Article 13 and 14 of the UK GDPR2. However, it may be good practice to do so, as well as to consult with individuals or their representatives, where appropriate, as part of the DPIA process. This can help to enhance transparency, trust and accountability, and to identify any additional risks or concerns from the perspective of the data subjects.Reference:

Article 35(7) of the UK GDPR1

Article 13 and 14 of the UK GDPR2

Question 10

Question Type: MultipleChoice

Of the following options which is NOT a purpose of carrying out a Data Protection Impact Assessment (DPIA)?

Options:

A- It is necessary to fulfil the requirement that all DPIAs are submitted to the ICO

B- It is key to the accountability element of the GDPR.

C- It fulfils a requirement that data protection is carried out by design and default.

D- It assists in identifying the main risks that may exist in any use of data, so that they can be mitigated

Answer:

A

Explanation:

A DPIA is not required to fulfil the requirement that all DPIAs are submitted to the ICO, because this is not a requirement under the GDPR. The GDPR only requires that the controller consults the ICO before carrying out processing that is likely to result in a high risk to individuals, if the controller cannot mitigate that risk. This means that not all DPIAs need to be submitted to the ICO, only those that identify a high residual risk that cannot be reduced. The other options are valid purposes of carrying out a DPIA, as they help the controller to comply with the GDPR, ensure data protection by design and by default, and identify and mitigate the main risks to individuals' rights and freedoms.Reference:

Article 35 and 36 of the GDPR3

ICO guidance on DPIAs5

Question 11

Question Type: MultipleChoice

What is the basis of the accountability and data governance obligation (Article 5 (2) of the GDPR)?

Options:

A- The controller shall appoint a DPO before carrying out large scale processing

B- The controller shall be responsible for. and be able to demonstrate compliance with the data protection principles.

C- Controllers and Processors each have a responsibility to conduct legitimate interests balancing tests before processing data for direct marketing

D- Processors have overarching responsibility to ensure their processing is compliant

Answer:

B

Explanation:

Article 5(2) of the GDPR introduces the principle of accountability, which requires that the controller is responsible for, and be able to demonstrate compliance with, the data protection principles set out in Article 5(1). These principles are: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and data protection by design and by default. The controller must implement appropriate technical and organisational measures to ensure and demonstrate compliance, such as policies, procedures, records, audits, reviews, and DPIAs. The controller must also cooperate with the supervisory authority and provide any information requested by it. The other options are not the basis of the accountability and data governance

obligation, although they may be related to other obligations under the GDPR.Reference:

Article 5(2) of the GDPR3

ICO guidance on accountability and governance4

Question 12

Question Type: MultipleChoice

Article 9(2)(c) of UK GDPR condition of processing special category data in the vital interests of the data subject is only applicable in which of the following circumstances:

Options:

A- When another lawful basis applies.

B- When a data subject is incapacitated

C- When the data subject is physically unable to be present

D- When the data subject refuses to consent

Answer:

B

Explanation:

Article 9(2) of UK GDPR allows the processing of special category data when it is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. This means that the data subject is unable to exercise their right to consent or object to the processing, either because they are unconscious, in a coma, suffering from a severe mental disorder, or otherwise unable to communicate their wishes. This condition is intended to cover emergency situations, such as life-threatening medical interventions, where the data subject's consent cannot be obtained in time. It does not apply when another lawful basis applies, when the data subject is physically absent but still capable of giving consent, or when the data subject refuses to consent.Reference:

Article 9(2) of UK GDPR1

ICO guidance on special category data2