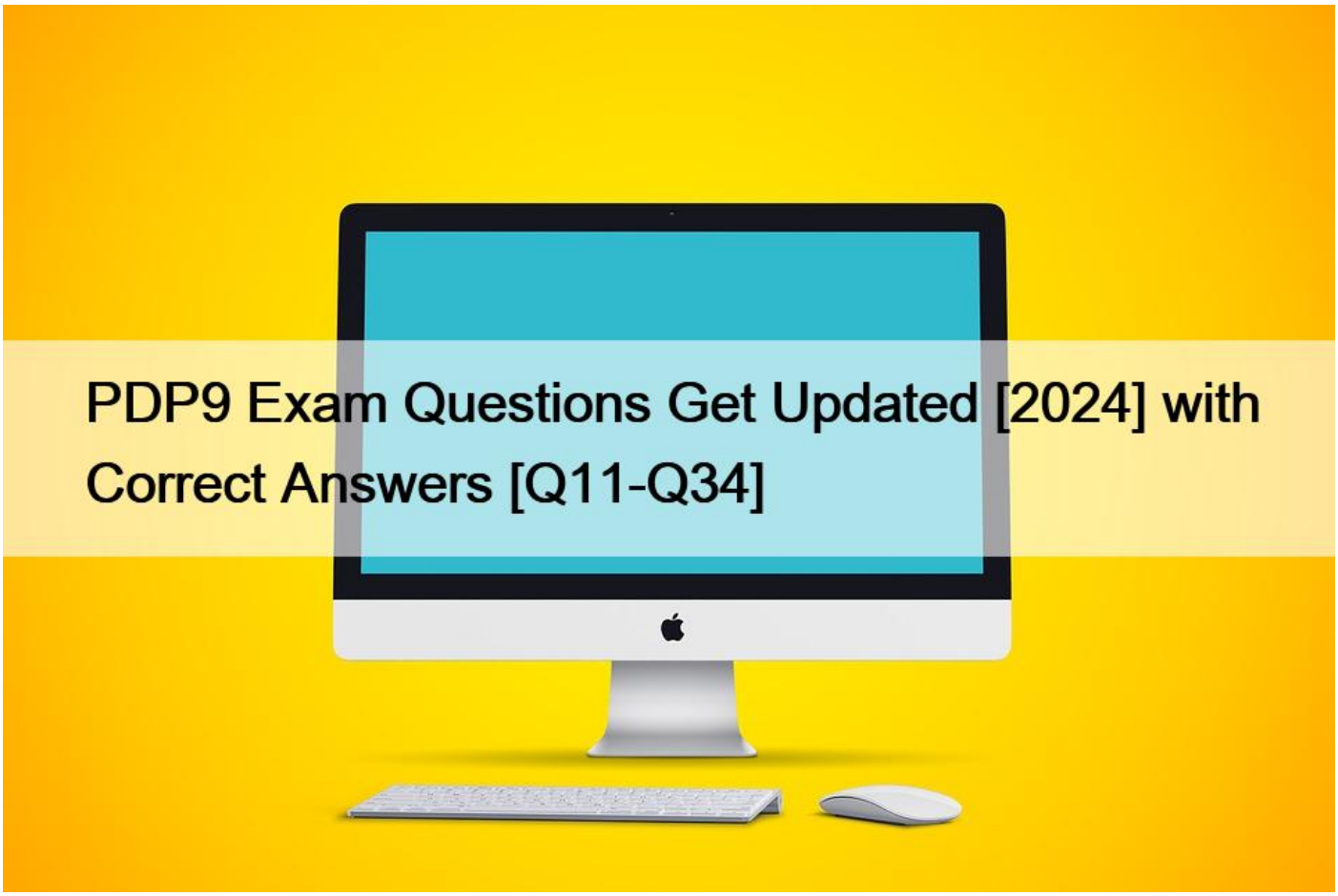
PDP9 Exam Questions Get Updated [2024 with Correct Answers [Q11-Q34



PDP9 Exam Questions Get Updated [2024] with Correct Answers
Practice PDP9 Questions With Certification guide Q&A from Training Expert ValidBraindumps

The PDP9 certification program covers a wide range of topics related to data protection and privacy, including GDPR, data protection principles, confidentiality, privacy impact assessments, and much more. PDP9 course material is delivered through classroom training, online learning resources, and self-study materials. Candidates for the PDP9 exam are required to have a working knowledge of data protection principles and practices, and they must demonstrate their understanding of relevant legislation, regulations and best practices in the field of data protection.

Q11. Which of the following is NOT a role of the Information Commissioner’s Office?
* Publishing a list of the kind of processing that is subject to the requirement for a DPIA
* Providing an annual activity report to Parliament
* Providing case by case advice on what retention period companies should use
* Encouraging the establishment of data protection certification mechanisms and of data protection seals
Explanation

The Information Commissioner’s Office (ICO) is the UK’s independent authority for data protection, which is responsible for upholding the UK GDPR and the Data Protection Act 2018, as well as other related legislation.

The ICO has various roles and tasks, such as monitoring and enforcing the application of the data protection law, promoting publicawareness and understanding of the risks and rights related to processing, advising the Parliament and the government on legislative and administrative measures concerning data protection, encouraging the development of codes of conduct and certification schemes, and handling complaints and investigations. However, the ICO does not provide case by case advice on what retention period companies should use, as this is a matter for the companies themselves to determine, based on their own purposes, legal obligations, and risk assessments. The ICO only provides general guidance on the data minimisation and storage limitation principles, which require that personal data should be kept only for as long as necessary and no longer than that. The ICO also expects companies to have clear policies and procedures on how they retain and dispose of personal data, and to document their retention periods and the reasons for them. References:

* Article 57 of the UK GDPR1

* ICO guidance on the role of the ICO2

* ICO guidance on data minimisation and storage limitation3

Q12. Under the Privacy and Electronic Communications Regulations, organisations must NOT make marketing telephone calls to which of the following?
* Any person under the age of 18, unless their parent or guardian has provided permission
* Any person who is registered with the Telephone Preference Service, unless they have given specific consent to receive your calls
* Any person who has not consented to receiving marketing calls
* Any person outside of the United Kingdom.

Explanation

The Privacy and Electronic Communications Regulations (PECR) are a set of rules that regulate the use of electronic communications for marketing purposes, such as phone calls, texts, emails and faxes. One of the rules is that organisations must not make unsolicited marketing calls to individuals who have registered their numbers with the Telephone Preference Service (TPS), unless they have given their prior consent to receive such calls from that organisation. The TPS is a free service that allows individuals to opt out of receiving any marketing calls. It is a legal requirement for organisations to check the TPS before making any marketing calls and to respect the preferences of the individuals registered on it. If an organisation fails to comply with this rule, it may face enforcement action from the Information Commissioner’s Office (ICO), which is the UK’s data protection authority and the regulator of PECR. References:

* Telephone Preference Service

* Marketing calls

* Enforcement action

Q13. What does NOT have an exemption prescribed under schedule 3 of the Data Protection Act 2018?
* Social Work Data.
* Credit checking agency data
* Education data, examination scripts and marks
* Health data

Q14. Article 57 of the UK GDPR states that the tasks of the Commissioner include -Select the INCORRECT answer
* Handling complaints raised by individuals/data subjects

* Providing general guidance to clarify the law.
* Adopting consistency findings in cross-border data protection cases
* Advising UK Parliament on issues related to the protection of personal data

Explanation

Article 57 of the UK GDPR states that the tasks of the Commissioner include handling complaints raised by individuals/data subjects, providing general guidance to clarify the law, and advising UK Parliament on issues related to the protection of personal data, among other tasks. However, adopting consistency findings in cross-border data protection cases is not a task of the Commissioner, but of the European Data Protection Board (EDPB), which is an independent body composed of the heads of the supervisory authorities of the EU and EEA member states and the European Data Protection Supervisor. The EDPB is responsible for ensuring the consistent application of the EU GDPR across the EU and EEA, and for issuing opinions and decisions on matters of general application or affecting more than one member state. The UK is no longer part of the EU or the EEA, and therefore the EDPB does not have jurisdiction over the UK GDPR or the Commissioner. The UK has its own mechanism for ensuring consistency and cooperation with other countries, which involves the Commissioner and the Secretary of State. References:

* Article 57 of the UK GDPR1

* Article 63 and 64 of the EU GDPR4

* ICO guidance on the UK GDPR and the EU GDPR5

Q15. A company has twenty retail outlets in France and thirty retail outlets in Belgium The payroll department and the Data Protection Officer are based in Poland.The Company Board and administrative functions are based in Germany. Determine where the company’s ‘mainestablishment’ would be

* Belgium
* France
* Germany
* Poland

Explanation

The main establishment of a controller or a processor in the EU is the place where the decisions on the purposes and means of the processing of personal data are taken and implemented. According to Recital 36 of the GDPR, the main establishment of a controller with establishments in more than one Member State should be the place of its central administration in the EU, unless the decisions on the processing are taken in another establishment of the controller in the EU and the latter establishment has the power to have such decisions implemented, in which case the establishment havingtaken such decisions should be considered to be the main establishment. Similarly, the main establishment of a processor with establishments in more than one Member State should be the place of its central administration in the EU, or, if the processor has no central administration in the EU, the establishment of the processor in the EU where the main processing activities take place to the extent that the processor is subject to specific obligations under the GDPR. The main establishment is relevant for determining the lead supervisory authority, the applicable law, and the jurisdiction of the courts for cross-border processing of personal data. In this case, the company’s main establishment would be Germany, as it is the place where the company board and administrative functions are based and where the decisions on the processing of personal data are likely to be taken and implemented.

References:

* Recital 36 of the GDPR8

* Article 4(16) of the GDPR9

* Article 56 of the GDPR

Q16. An individual applies for a job as a security guard The employer has had significant issues with the sickness record of past recruits They therefore decide to offer the position to the individual on the basis they request a copy of their medical record so that the employer can be assured that they are in a good state of health.

The Data Protection Officer has been asked to advise. What advice is MOST appropriate?
* Providing the medical evidence is used for a legitimate purpose, and that the information is securely destroyed on verification that the employee is healthy, this is an acceptable action.
* While requesting and viewing medical evidence may be legitimate, they should ask for evidence that the individual consents to the proposition that they make the request
* In requesting information that is more than they necessary require to verify the medical condition of the individual they will have breached the data minimisation principle
* This is a criminal offence under the Data Protection Act 2018 No individual should be asked to make a subject access request in order to obtain health records in these circumstances.

Explanation

The Data Protection Act 2018 (DPA 2018) makes it a criminal offence for a person to require another person to make a subject access request for information about their health, convictions or cautions, or spent convictions, and to provide that information to the first person or a third person, as a condition of providing or offering to provide goods, facilities or services, or as a condition of entering into or continuing a contract. This is known as an enforced subject access request. The employer in this scenario is committing a criminal offence by offering the job to the individual on the condition that they request a copy of their medical record and provide it to the employer. The employer is also breaching the data protection principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, and storage limitation, as they are processing health data, which is a special category of personal data, without a valid legal basis, without informing the individual of the purpose and legal basis of the processing, and without limiting the processing to what is necessary and relevant for the employment relationship. The employer should instead obtain the individual’s explicit consent to request the health information directly from the relevant health professional, and only request the information that is necessary and proportionate for the specific role of a security guard. References

:

* Section 184 of the DPA 20183

* ICO guidance on enforced subject access requests4

* ICO guidance on special category data5

Q17. 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:
* When another lawful basis applies.
* When a data subject is incapacitated
* When the data subject is physically unable to be present
* When the data subject refuses to consent

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. References:

* Article 9(2) of UK GDPR1

* ICO guidance on special category data2

Q18. What does NOT have an exemption prescribed under schedule 3 of the Data Protection Act 2018?
* Education data, examination scripts and marks
* Credit checking agency data
* Social Work Data.
* Health data

Explanation

Schedule 3 of the Data Protection Act 2018 (DPA 2018) provides exemptions from some of the UK GDPR provisions for certain types of personal data processing, such as health data, social work data, education data, and child abuse data. These exemptions are intended to balance the rights and freedoms of data subjects with the public interest or the legitimate interests of data controllers in specific contexts. For example, the exemptions may allow data controllers to restrict the data subjects’ access to their personal data, or to process their personal data without their consent, if complying with the UK GDPR would be likely to prejudice the purposes of the processing, such as the provision of health care, social work, education, or child protection.

However, Schedule 3 of the DPA 2018 does not provide any exemption for credit checking agency data, which is personal data processed by credit reference agencies for the purposes of assessing the creditworthiness of individuals or organisations, or preventing fraud or money laundering. Credit checking agency data is subject to the UK GDPR provisions as normal, unless another exemption applies. For example, credit reference agencies may rely on the crime and taxation exemption in Schedule 2, Part 1, Paragraph 2 of the DPA 2018 if disclosing personal data to a data subject would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders. References:

* Data Protection Act 2018, Schedule 31

* ICO Guide to Data Protection, Exemptions2

* ICO Guide to Data Protection, Credit3

Q19. What are Information Society Services’? Select the INCORRECT answer
* A service provided for remuneration, by electronic means, at distance to an individual that has requested it.
* An electronic information service provided to individuals but paid for solely by advertising
* Business to business online networking sites
* Information services provided by non-profit or government organisations with no remuneration

Explanation

Information society services (ISS) are defined in Article 4(25) of the UK GDPR as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services”. This means that ISS are online services that are paid for, either by the user or by another source of income, such as advertising or sponsorship, and that are provided without the parties being physically present, using electronic equipment for the transmission and reception of data, and upon the request of the user.

Examples of ISS include apps, programs, websites, search engines, social media platforms, online marketplaces, content streaming services, online games, and any other online services that offer goods or services to users over the internet. Therefore, options A, B and C are correct examples of ISS, as they meet the criteria of the definition. However, option D is not a correct example of ISS, as it does not involve any remuneration for the service provider. Information services provided by non-profit or government

organisations with no remuneration are not considered ISS under the UK GDPR, unless they compete with other ISS on the market. References:

* UK GDPR, Article 4(25)4

* Services covered by this code5

Q20. What is the meaning of storage limitation in relation to UK GDPR Article 5 (1)(e)?
* Keeping identifiable personal data for no longer than is necessary for the intended processing
* Storing data in a secure format only permitting access to those with a business need
* Only storing data in locations within the EU. except where there is an adequacy decision.
* Limiting the number of records stored in any single repository to minimise risk surface.
Explanation

Storage limitation is one of the principles of data protection under the UK GDPR. It means that personal data should not be kept in a form that allows identification of data subjects for longer than is necessary for the purposes for which the data are processed. The UK GDPR does not specify any fixed time limits for different types of data, but rather requires data controllers to determine and justify the appropriate retention periods for their processing activities, taking into account factors such as the nature, scope, context and purposes of the processing, the risks to the rights and freedoms of data subjects, and the legal obligations and expectations of the data controller. Data controllers should also have a policy setting out standard retention periods where possible, and review the data they hold regularly to ensure that it is erased or anonymised when it is no longer needed. Data subjects have the right to request the erasure of their personal data if the data controller no longer has a lawful basis or a legitimate interest for keeping it. The UK GDPR allows for some exceptions to the storage limitation principle, such as when the personal data is processed solely forarchiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to appropriate safeguards for the rights and freedoms of data subjects. References:

* UK GDPR, Article 5 (1) (e) and (2)4

* UK GDPR, Article 175

* UK GDPR, Article 896

* ICO Guide to Data Protection, Storage Limitation7

Q21. Describe the act of processing under the authority of a controller or processor as stipulated in UK GDPR Article 29.
* 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.
* A processor shall not process those data except on instructions from the controller, unless required to do so by domestic law
* 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.
* 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.
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). References:

* Article 29 of UK GDPR1

* ICO guidance on controllers and processors2

Q22. Which of the following statements MOST accurately describes why a risk-based approach to the use of Al is necessary?
* Al is inherently negative and its use should be limited
* Al is unlawful
* Al’s benefits make accepting all arising risks necessary.
* Al carries new and complex risks not present in other technologies

Explanation

Artificial intelligence (AI) is the use of digital systems to perform tasks that would normally require human intelligence, such as recognition, decision making, learning and adaptation. AI can bring many benefits to society, such as innovation, efficiency, personalisation and convenience. However, AI also carries new and complex risks that are not present in other technologies, such as opacity, unpredictability, bias, discrimination, intrusion, manipulation and harm. These risks can affect the rights and freedoms of individuals, especially their data protection rights, such as privacy, transparency, fairness, accuracy and accountability. Therefore, a risk-based approach to the use of AI is necessary, which means identifying, assessing and mitigating the potential adverse impacts of AI on individuals and society, while balancing them with the benefits and opportunities. A risk-based approach also means complying with the relevant legal and ethical frameworks, such as the UK GDPR and the DPA 2018, and following the best practices and guidance issued by the ICO and other authorities on AI and data protection234. References:

* Guidance on AI and data protection2

* Explaining decisions made with AI3

* AI auditing framework4

Q23. 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 ImpactAssessment C It is mandatory for all data processors D The controller or the processor a mustmakesthe record available to the supervisory authority on request

E. It must contain contact details for the supervisory authority
* B, C. and D
* A,C,andE
* A. C,D, and E
* A, C,andD

Explanation

Article 30 of the UK GDPR3 requires 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. References:

* Article 30 of the UK GDPR3

* Article 35 of the UK GDPR4

Q24. If a complainant disagrees with the decision of the UK’s supervisory authority, how do they appeal this decision?
* To the First Tier Tribunal (Information Rights)
* To the Information Commissioner
* To the European Data Protection Supervisor.
* To the European Commission
Explanation

If a complainant disagrees with the decision of the UK’s supervisory authority, which is the Information Commissioner’s Office (ICO), they have the right to appeal to the First Tier Tribunal (Information Rights).

The tribunal is an independent body that can review the ICO’s decision and either uphold it, vary it or cancel it. The tribunal can also direct the ICO to take certain actions, such as issuing a decision notice or an enforcement notice. The appeal must be lodged within 28 days of receiving the ICO’s decision, using the notice of appeal form and providing the relevant documents and grounds for appeal. The tribunal will then notify the ICO and the complainant of the appeal and the procedure for dealing with it. The tribunal may hold a hearing to examine the evidence and arguments of both parties, or decide the case on the basis of written submissions only. The tribunal will issue a written decision, which will be sent to both parties and published on the tribunal’s website. The tribunal’s decision can be further appealed tothe Upper Tribunal on a point of law, with the permission of the First Tier Tribunal or the Upper Tribunal. References:

* Information rights and data protection: appeal against the Information Commissioner1

* Notice of appeal form2

* First Tier Tribunal (Information Rights) website3

Q25. Of the following options which is NOT a purpose of carrying out a Data Protection Impact Assessment (DPIA)?
* It is necessary to fulfil the requirement that all DPIAs are submitted to the ICO

* It is key to the accountability element of the GDPR.
* It fulfils a requirement that data protection is carried out by design and default.
* It assists in identifying the main risks that may exist in any use of data, so that they can be mitigated

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 highrisk 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. References:

* Article 35 and 36 of the GDPR3

* ICO guidance on DPIAs5

Q26. Of the following options which is NOT a purpose of carrying out a Data Protection Impact Assessment (DPIA)?
* It assists in identifying the main risks that may exist in any use of data, so that they can be mitigated
* It is necessary to fulfil the requirement that all DPIAs are submitted to the ICO
* It fulfils a requirement that data protection is carried out by design and default.
* It is key to the accountability element of the GDPR.

Q27. 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’?
* They are controllers of their own information contained in the single order system only
* 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.
* The businesses are controllers of their respective information, and the staff are processors of this information
* They are both joint controllers of the information contained in the single order system

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. References:

* Article 26 of the GDPR1

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

Prepare Top BCS PDP9 Exam Audio Study Guide Practice Questions Edition:
https://www.validbraindumps.com/PDP9-exam-prep.html]