Free Questions for PDP9 by actualtestdumps

Shared by Burke on 18-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following statements MOST accurately describes the potential impact of AI on the principle of transparency?

Options:

A- Data subjects should generally expect AI to be present in processing activities

B- Transparency requirements do not apply to AI, as it is always compatible with original purposes

C- AI can lead to invisible processing, with data subjects not being aware of its presence.

D- Transparency requirements do not apply to AI, as there is a relevant exemption

Answer:

C

Explanation:

The principle of transparency requires that any processing of personal data is fair, lawful and transparent to the data subjects. This means that data subjects should be informed about the existence, nature, purpose and consequences of the processing, as well as their

rights and choices regarding their data. Transparency is essential for ensuring accountability, trust and compliance in data processing. However, the use of AI can pose challenges to the principle of transparency, as AI can lead to invisible processing, with data subjects not being aware of its presence, or the logic, significance and implications of the processing. For example, AI can be used to profile, infer, predict or influence the behaviour, preferences, interests, emotions or personality of data subjects, without their knowledge or consent. AI can also be used to make automated decisions that affect data subjects, such as credit scoring, recruitment, health diagnosis or social benefits, without providing meaningful explanations or opportunities for human intervention.Therefore, it is important to ensure that data subjects are informed and empowered when AI is involved in the processing of their data, and that they can exercise their rights, such as the right to access, rectify, object, restrict, erase or port their data, or the right to challenge or contest automated decisions56.Reference:

Guidance on AI and data protection5

Explaining decisions made with AI6

Question 2

Question Type: **MultipleChoice**

Which of the following statements MOST accurately describes why a risk-based approach to the use of AI is necessary?

Options:

A- AI is inherently negative and its use should be limited

B- AI is unlawful

C- AI's benefits make accepting all arising risks necessary.

D- AI carries new and complex risks not present in other technologies

Answer:

D

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.Reference:

Guidance on AI and data protection2

Explaining decisions made with AI3

Question 3

Question Type: MultipleChoice

How are data sharing practices governed by data protection law?

Options:

A- Data sharing practices are covered in the DPA 2018, supported by a statutory Code of Practice that provides specific guidance

B- Data sharing practices are subject to the PECR until the new statutory Code of Practice is published

C- Data sharing practices are covered by the Freedom of Information Act

D- Data sharing practices are not specifically regulated, however the ICO provide best practice guidance

Answer:

A

Explanation:

Data sharing is the disclosure of personal data from one or more organisations to a third party organisation or organisations, or the sharing of personal data within an organisation. Data sharing practices are governed by data protection law, which includes the UK GDPR and the Data Protection Act 2018 (DPA 2018). The DPA 2018 contains specific provisions on data sharing, such as the power of the Information Commissioner's Office (ICO) to issue a statutory Code of Practice on data sharing.The ICO has published a Data Sharing Code of Practice1that provides practical guidance on how to share data in a fair, safe and transparent way, in compliance with the data protection principles and the rights of data subjects. The code is not legally binding, but it reflects the ICO's interpretation of the law and it may be used as evidence in legal proceedings or investigations. The code also contains useful tools, case studies and examples that can help organisations to share data effectively and responsibly.Reference:

Data Sharing Code of Practice1

Question 4

Question Type: MultipleChoice

How does the GDPR relate to cookies?

Options:

A- The GDPR only applies where a cookie processes personal data

B- The GDPR applies in all cases where cookies are used

C- Where PECR is engaged only PECR will apply to the processing of personal data

D- Websites only need an opt out of cookies if GDPR applies

Answer:

C

Explanation:

The GDPR and the Privacy and Electronic Communications Regulations (PECR) are two different but related legal frameworks that regulate the use of cookies and similar technologies. Cookies are small text files that are stored on the user's device when they visit a website or use an online service. Cookies can be used for various purposes, such as remembering user preferences, tracking user behaviour, delivering targeted advertising, or enabling online transactions. The GDPR applies to the processing of personal data by cookies and similar technologies, as they can be used to identify or single out individuals, either directly or indirectly. Personal data is any information relating to an identified or identifiable natural person, such as a name, an email address, a location data, or a cookie identifier. The GDPR requires data controllers to obtain the user's consent before using any cookies that are not strictly necessary for the functioning of the website or service, and to provide clear and transparent information about the purposes and legal basis of the processing, the categories and recipients of the personal data, the retention periods, and the rights of the data subjects. The GDPR also requires data controllers to implement appropriate technical and organisational measures to ensure the security and confidentiality of the personal data, and to comply with the principles of data protection by design and by default. The PECR are a set of UK-specific rules that implement the EU ePrivacy Directive, which is a complementary legislation to the GDPR that deals with the privacy and security of

electronic communications. The PECR apply to the use of cookies and similar technologies, as well as to the sending of marketing communications by phone, email, text, or fax, and to the provision of public electronic communications services and networks. The PECR require data controllers to obtain the user's consent before using any cookies or similar technologies, except those that are strictly necessary for the provision of an information society service requested by the user, or for the sole purpose of carrying out the transmission of a communication over an electronic communications network. The PECR also require data controllers to provide clear and comprehensive information about the purposes of the cookies or similar technologies, and to offer the user a way to refuse or withdraw their consent. The PECR do not apply to the processing of personal data by cookies or similar technologies, as this is covered by the GDPR. Therefore, the correct answer is C, as where PECR is engaged only PECR will apply to the use of cookies or similar technologies, but not to the processing of personal data by them. The other options are incorrect because:

The GDPR does not only apply where a cookie processes personal data, but to any processing of personal data by any means, including cookies and similar technologies. The GDPR applies to the processing of personal data by cookies and similar technologies, regardless of whether they are strictly necessary or not, or whether they are first-party or third-party cookies. However, the GDPR does not apply to the use of cookies or similar technologies, as this is covered by the PECR.

The GDPR does not apply in all cases where cookies are used, but only in cases where cookies are used to process personal data. The GDPR does not apply to the use of cookies or similar technologies that do not process personal data, such as those that are strictly necessary for the functioning of the website or service, or those that do not identify or single out individuals. However, the PECR still apply to the use of cookies or similar technologies, regardless of whether they process personal data or not, except for some limited exemptions.

Websites do not only need an opt out of cookies if GDPR applies, but also if PECR applies. The GDPR and the PECR both require data controllers to obtain the user's consent before using any cookies or similar technologies that are not strictly necessary, and to offer the user a way to refuse or withdraw their consent. The opt out of cookies is a mechanism that allows the user to exercise their right to object to the use of cookies or similar technologies, and to prevent the processing of their personal data by them. Websites need to provide an opt out of cookies in all cases where the user's consent is required, regardless of whether the GDPR or the PECR

applies.Reference:

GDPR, Article 4(1)5

GDPR, Article 6(1)(a)6

GDPR, Article 13 and 147

GDPR, Article 328

GDPR, Article 25

PECR, Regulation 6

PECR, Regulation 5

Question 5

Question Type: **MultipleChoice**

In the terms of their relevance under data protection legislation, how can CCTV images recorded in a supermarket BEST be described'?

Options:

A- They are special category data as they identify special characteristics

B- They are biometric data in the terms of the definition stipulated in the GDPR.

C- The GDPR is only engaged where these are accompanied by text or other identifier

D- They are personal data as they can be used to identify living human beings

Answer:

D

Explanation:

CCTV images recorded in a supermarket are personal data as they can be used to identify living human beings, either directly or indirectly, by their physical appearance, clothing, accessories, or other distinctive features. Personal data is defined in Article 4(1) of the GDPR as "any information relating to an identified or identifiable natural person". The GDPR applies to the processing of personal data by automated means, such as CCTV cameras, or by non-automated means that form part of a filing system, such as paper records. The other options are incorrect because:

CCTV images are not special category data as they do not reveal any of the sensitive information listed in Article 9(1) of the GDPR, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, or biometric or genetic data. Special category data is subject to stricter conditions and safeguards under the GDPR, as it poses a higher risk to the rights and freedoms of individuals.

CCTV images are not biometric data in the terms of the definition stipulated in the GDPR. Biometric data is defined in Article 4(14) of the GDPR as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". CCTV images do not result from specific technical processing, nor do they allow or confirm the unique identification of a natural person, unless they are combined with other data or identifiers.

The GDPR is not only engaged where CCTV images are accompanied by text or other identifier. The GDPR applies to any information that relates to an identified or identifiable natural person, regardless of whether it is accompanied by text or other identifier. CCTV images can relate to an identifiable natural person even if they do not contain any text or other identifier, as long as there is a possibility to single out or link the person to other data or factors.Reference:

GDPR, Article 4(1)1

GDPR, Article 2(1)2

GDPR, Article 9(1)3

GDPR, Article 4(14)4

Question 6

Question Type: **MultipleChoice**

What is the Employment Practices Code?

Options:

A- Guidance on meeting legal requirements of data protection when employing staff

B- Guidance on the requirements for employing a Data Protection Officer

C- A statutory framework for implementing data protection training for employees.

D- A set of exemptions that can be used when processing data related to employees

Answer:

A

Explanation:

The Employment Practices Code is a guidance document issued by the ICO that provides recommendations on how to comply with the data protection principles and the rights of data subjects when processing personal data in the context of employment. The code covers various aspects of employment practices, such as recruitment and selection, employment records, monitoring at work, and information about workers' health. The code is not legally binding, but it reflects the ICO's interpretation of the Data Protection Act and the UK GDPR, and it may be used as evidence in legal proceedings or investigations. The code is intended to help employers balance their legitimate interests in managing their workforce with the privacy rights of their workers.Reference:

The Employment Practices Code

Quick Guide to the Employment Practices Code

Question 7

Question Type: MultipleChoice

Under the Privacy and Electronic Communications Regulations, organisations must NOT make marketing telephone calls to which of the following?

Options:

A- Any person under the age of 18, unless their parent or guardian has provided permission

B- Any person who is registered with the Telephone Preference Service, unless they have given specific consent to receive your calls

C- Any person who has not consented to receiving marketing calls

D- Any person outside of the United Kingdom.

Answer:

B

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.Reference:

Telephone Preference Service

Marketing calls

Enforcement action

Question 8

Question Type: **MultipleChoice**

In which of the following circumstances would Privacy and Electronic Communications Regulation (PECR) NOT apply?

Options:

A- Telephone marketing communications

B- Postal marketing communications.

C- Text marketing communications.

D- Email marketing communications

Answer:

B

Explanation:

The Privacy and Electronic Communications Regulations (PECR) are a set of rules that regulate the use of electronic communications for marketing purposes, as well as the use of cookies and similar technologies, and the security and privacy of electronic communications services. PECR apply to all organisations that market by phone, email, text, fax, or online, or that use cookies or similar technologies on their websites or other electronic services. PECR do not apply to postal marketing communications, which are not considered electronic communications under the definition of PECR. However, postal marketing communications may still be subject to the UK GDPR and the Data Protection Act 2018, as well as other regulations, such as the Consumer Protection from Unfair Trading Regulations 2008 and the Advertising Standards Authority codes of practice.Reference:

ICO Guide to PECR, What are PECR?4

ICO Guide to PECR, Electronic and telephone marketing5

Question 9

Question Type: MultipleChoice

What does NOT have an exemption prescribed under schedule 3 of the Data Protection Act 2018?

Options:

A- Education data, examination scripts and marks

B- Credit checking agency data

C- Social Work Data.

D- Health data

Answer:

B

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.Reference:

Data Protection Act 2018, Schedule 31

ICO Guide to Data Protection, Exemptions2

ICO Guide to Data Protection, Credit3

Question 10

Question Type: **MultipleChoice**

In which of the following circumstances does a public authority NOT need to appoint a Data Protection Officer?

Options:

A- Where it processes a large amount of personal data

B- Where it is a court acting in its judicial capacity

C- Where it processes special category data

D- Where it is defined as a public body in the Data Protection Act 2018

Answer:

B

Explanation:

Under Article 37 of the UK GDPR, a public authority or a public body must appoint a data protection officer (DPO) unless it is a court acting in its judicial capacity. This is the only exception for public authorities or bodies from the obligation to appoint a DPO. The other circumstances listed in the question, such as processing a large amount of personal data, processing special category data, or being defined as a public body in the Data Protection Act 2018, do not exempt a public authority or a public body from appointing a DPO.Reference:

Article 37 of the UK GDPR2

Data protection officers | ICO2

Question 11

Question Type: MultipleChoice

Where are the definitions of "Public Authority" and "Public Bodies" found?

Options:

A- Freedom of Information Act 2000 and Data Protection Act 2018

B- GDPR and Data Protection Act 2018.

C- Data Protection Act 2018 and PECR.

D- Data Protection Act 2018 only

Answer:

A

Explanation:

The definitions of "public authority" and "public body" for the purposes of the UK GDPR and the Data Protection Act 2018 are found in the Freedom of Information Act 2000 and the Data Protection Act 2018 respectively. Section 7 of the Data Protection Act 2018 provides

that a public authority or a public body is one that is listed in Schedule 1 to the Freedom of Information Act 2000, or is designated by an order under section 5 of that Act. However, a court or tribunal acting in its judicial capacity is not considered a public authority or a public body under the Data Protection Act 2018.Reference:

Section 7 of the Data Protection Act 20181

Schedule 1 to the Freedom of Information Act 2000