Free Questions for PDP9

Shared by Rios on 16-04-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the below would be the BEST example of processing that could utilise the Public Interest Task lawful basis?

Options:

A- A health authority processing the personal information of its staff in order to record all training undertaken
B- A debt collection agency processing information relating to unpaid fines for misuse of community council car parking.
C- A local authority processing the personal information of the person responsible for paying council tax
D- A tax authority drops cookies on the devices of visitors to its website

Answer:

C

Explanation:

The public interest task lawful basis applies to the processing of personal data that 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. The relevant task or authority must have a clear basis in domestic law, such as a statutory power, a common law duty, or a function of the Crown, central or local government. The processing must also be necessary, meaning that there is no reasonable and less intrusive way to achieve the same purpose. The public interest task lawful basis is most relevant to public authorities, but it can also apply to any organisation that exercises official authority or carries out tasks in the public interest. In scenario C, a local authority processing the personal information of the person responsible for paying council tax is likely to rely on the public interest task lawful basis, as it is performing a task in the public interest that is laid down by law, namely the Local Government Finance Act 1992, and the processing is necessary for the collection and administration of council tax. In contrast, scenarios A, B and D are less likely to qualify for the public interest task lawful basis, as they do not involve a clear task or authority that is set out in law, or that serves the public interest. For example, a health authority processing the personal information of its staff in order to record all training undertaken may have a different lawful basis, such as legitimate interests or contractual necessity. A debt collection agency processing information relating to unpaid fines for misuse of community council car parking may not have any official authority or public interest justification for its processing. A tax authority dropping cookies on the devices of visitors to its website may not be able to demonstrate that the processing is necessary for its official functions, and may

also need to comply with the Privacy and Electronic Communications Regulations (PECR) for the use of cookies.Reference:

UK GDPR, Article 6 (1) (e) and (3)8

ICO Guide to Data Protection, Public Task9

Local Government Finance Act 199210

Question 2

Question Type: MultipleChoice

Who is entitled to a private life by law in the UK?

Options:

A- All individuals.
B- All individuals save for Members of Parliament
C- Private individuals who do not conduct their business on public platforms (such as professional sports people and actors
D- Nobody

Answer:

A

Explanation:

The right to a private life is a fundamental human right that is protected by law in the UK. Article 8 of the European Convention on Human Rights (ECHR), which is incorporated into UK law by the Human Rights Act 1998, states that ''Everyone has the right to respect for his private and family life, his home and his correspondence''. This right applies to all individuals, regardless of their status, profession, or public exposure. The right to a private life covers aspects such as personal identity, personal relationships, physical and mental well-being, personal data, and correspondence. However, this right is not absolute and can be limited or interfered with by the state or other parties in certain circumstances, such as for the protection of national security, public safety, health, morals, or the rights and freedoms of others.Reference:

Article 8 of the ECHR1

Human Rights Act 19982

ICO Guide to Data Protection3

Question 3

Question Type: MultipleChoice

An investigation reveals that an individual is defrauding a public authority After a (suspected) tip off from a senior manager, the individual submits a Subject Access Request to the authority asking for a copy of all personal data relating to any investigations that have been carried out

What would be the BEST approach?

Options:

A- The legal and professional privilege exemption applies to this information, and therefore the information does not need to be disclosed
B- They do not need to disclose details of the investigation as they can rely on the crime and taxation exemption on the basis that disclosure would prejudice the investigation
C- This is criminal offence data and therefore under the provisions of the Data Protection Act 2018, there is no obligation to disclose
D- While the right to inform does not apply in relation to criminal acts, they need to disclose the information as this has not yet been passed to the police.

Answer:

B

Explanation:

The crime and taxation exemption in Schedule 2, Part 1, Paragraph 2 of the Data Protection Act 2018 (DPA 2018) provides an exemption from the UK GDPR's transparency obligations and most individual rights, including the right of access, but only if complying with them would prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders. This means that the public authority does not need to disclose details of the investigation to the individual who submitted the subject access request, as doing so would be likely to hinder the investigation and enable the individual to evade justice. The public authority should assess the likelihood of prejudice on a case-by-case basis and document its reasons for relying on the exemption. The other options are incorrect because:

The legal and professional privilege exemption in Schedule 2, Part 1, Paragraph 19 of the DPA 2018 applies to personal data that is subject to an obligation of confidentiality arising from the

provision of legal advice or legal representation, or from the conduct of legal proceedings. This exemption does not apply to the information held by the public authority about the investigation, as it is not related to any legal advice or representation, or any legal proceedings.

The term ''criminal offence data'' refers to personal data relating to criminal convictions and offences, or related security measures. This type of data is subject to specific rules under Article 10 of the UK GDPR and Part 3 of the DPA 2018. However, this does not mean that there is no obligation to disclose criminal offence data in response to a subject access request. The public authority still needs to consider whether any of the exemptions in the DPA 2018 apply, such as the crime and taxation exemption, before disclosing or withholding the data.

The right to be informed does apply in relation to criminal acts, as the UK GDPR requires controllers to provide data subjects with information about the processing of their personal data, including the purposes and legal basis of the processing, unless an exemption applies. The fact that the information has not yet been passed to the police does not affect the applicability of the right to be informed or the right of access.Reference:

Data Protection Act 2018, Schedule 2, Part 1, Paragraph 21

ICO Guide to Data Protection, Crime and Taxation2

Data Protection Act 2018, Schedule 2, Part 1, Paragraph 193

UK GDPR, Article 104

Data Protection Act 2018, Part 35

UK GDPR, Article 13 and 146

Question 4

Question Type: MultipleChoice

Under the Privacy and Electronic Communications Regulations, organisations must NOT make marketing telephone calls to Which option best?

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 5

Question Type: MultipleChoice

A UK public body has a security breach, in which the details of a hundred thousand members of the public are published What is the MAXIMUM fine that they could receive for this breach?

Options:

A- 17 5 million or 4% of gross annual turnover
B- 10 million or 4% of gross annual turnover
C- 20 million or 2% of gross annual turnover
D- 8.7 million or 2% of gross annual turnover

Answer:

A

Explanation:

The UK GDPR and the Data Protection Act 2018 set a maximum fine of 17.5 million or 4% of annual global turnover, whichever is higher, for infringements of the data protection principles, the rights of data subjects, or the rules on transfers of personal data to third countries. This is the higher maximum penalty that applies to the most serious breaches of the UK GDPR. A security breach that exposes the details of a hundred thousand members of the public would likely fall under this category, as it would compromise the confidentiality and integrity of personal data, and potentially cause significant harm and distress to the data subjects. Therefore, the maximum fine that the UK public body could receive for this breach is 17.5 million or 4% of gross annual turnover, whichever is higher.Reference:

Penalties3

GDPR Penalties & Fines4

Three years of GDPR: the biggest fines so far5

Question 6

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 7

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 8

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 9

Question Type: MultipleChoice

When were data protection rights first introduced into UK law'?

Options:

A- 2000 (Data Protection Act 1998)
B- 1992 (Data Protection Act 1992).
C- 1984 (Data Protection Act 1984).
D- 2018 (Data Protection Act 2018)

Answer:

C

Explanation:

Data protection rights were first introduced into UK law by the Data Protection Act 1984, which was enacted to implement the Council of Europe Convention for the Protection of Individuals with

regard to Automatic Processing of Personal Data of 1981. The Data Protection Act 1984 established a set of principles for the processing of personal data by data users, such as obtaining consent, ensuring accuracy, and limiting retention. It also created a system of registration for data users and a Data Protection Registrar (later renamed as the Information Commissioner) to oversee and enforce the law. The Data Protection Act 1984 was replaced by the Data Protection Act 1998, which transposed the EU Data Protection Directive 1995 into UK law and extended the scope of data protection to cover manual as well as automated processing of personal data. The Data Protection Act 1998 was further amended by the Data Protection Act 2018, which incorporated the EU General Data Protection Regulation (GDPR) and the Law Enforcement Directive into UK law and made provisions for specific processing situations, such as national security, immigration, and journalism.Reference:

Data Protection Act 19844

Council of Europe Convention 1085

Data Protection Act 19986

Data Protection Act 20187

Question 10

Question Type: MultipleChoice

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 'main establishment' would be

Options:

A- Belgium
B- France
C- Germany
D- Poland

Answer:

C

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 having taken 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.Reference:

Recital 36 of the GDPR8

Article 4(16) of the GDPR9

Article 56 of the GDPR