Number: PDP9
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: PDP9

Exam Name: BCS Practitioner Certificate In Data Protection

Exam A

QUESTION 1
Which of the following would NOT be a personal data breach'?

A. The accidental deletion of an organisation's information security policy from the public facing website
B. The unauthorised changing of a persons address details on a database of customers.
C. The accidental destruction of a current employee's HR file.
D. The loss of a memory stick containing the names and addresses of students in private accommodation

Correct Answer: A
Section:
Explanation:
A personal data breach is defined in Article 4(12) of the UK GDPR as ''a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed''. Personal data means any information relating to an identified or identifiable natural person, such as a name, an identification number, location data, an online identifier or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Therefore, a personal data breach only occurs when the security incident affects personal data, not any other type of information. In this case, the accidental deletion of an organisation's information security policy from the public facing website would not be a personal data breach, as the policy does not contain any personal data. However, the other scenarios would be considered personal data breaches, as they involve the loss, alteration, destruction or unauthorised access to personal data of customers, employees or students.Reference:
UK GDPR, Article 4(12)1
UK GDPR, Article 4(1)2
ICO Guide to Data Protection, Personal Data Breaches3

QUESTION 2
How does the GDPR relate to cookies?

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

Correct Answer: C
Section:
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 3
How are data sharing practices governed by data protection law?

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

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

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

Correct Answer: D
Section:
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
AI auditing framework4

QUESTION 5
When does a personal data breach need to be reported to a supervisory authority?

A. All personal data breaches must be reported to a supervisory authority
B. Only where a disclosure is of special category data
C. Where the personal data breach is likely to result in a risk to the rights and freedoms of natural persons.
D. When the controller's right of freedom of expression outweighs the data subject's right to a private home and family life.

Correct Answer: C
Section:
Explanation:
Article 33 of the UK GDPR requires controllers to notify the supervisory authority of a personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. This means that not all personal data breaches need to be reported to the supervisory authority, only those that pose a risk to individuals. The risk should be assessed in terms of the potential negative consequences for individuals, such as discrimination, identity theft, fraud, financial loss, damage to reputation, loss of confidentiality, or any other significant economic or social disadvantage. The UK GDPR also requires controllers to communicate the personal data breach to the affected data subjects without undue delay, where the breach is likely to result in a high risk to their rights and freedoms. The other options are incorrect because:
The UK GDPR does not require all personal data breaches to be reported to the supervisory authority, only those that pose a risk to individuals. However, controllers must document all personal data breaches, regardless of whether they are reported or not, as part of their accountability obligations.
The UK GDPR does not make a distinction between personal data and special category data when it comes to reporting personal data breaches. Special category data is a type of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or that concerns health, sex life or sexual orientation, or biometric or genetic data for the purpose of uniquely identifying a natural person. The processing of special category data is subject to stricter conditions and safeguards under the UK GDPR, but the reporting of personal data breaches involving such data is subject to the same criteria as any other personal data breach, namely the risk to individuals.
The UK GDPR does not provide an exemption from reporting personal data breaches based on the controller's right of freedom of expression. The right of freedom of expression is a fundamental right that is recognised and protected by the UK GDPR, but it is not an absolute right that overrides the rights and freedoms of data subjects. The UK GDPR allows Member States to provide for exemptions or derogations from certain provisions of the UK GDPR for the processing of personal data carried out for journalistic purposes or the purpose of academic, artistic or literary expression, where such exemptions or derogations are necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information. However, these exemptions or derogations do not apply to the obligation to report personal data breaches to the supervisory authority, unless the Member State law specifies otherwise.Reference:
UK GDPR, Article 334
UK GDPR, Article 34
UK GDPR, Article 9
UK GDPR, Article 85

QUESTION 6
Which one task are supervisory authorities NOT required to carry out under Article 57(1)(f) of the UK GDPR? Select the CORRECT answer.

A. Handle complaints lodged by a data subject
B. Investigate complaints and inform the complainant of the progress of their investigation
C. Mediate between the complainant and the entity against which the complaint has been lodged, to resolve the complaint
D. Co-ordinate where necessary with other supervisory authorities

Correct Answer: C

Section:
Explanation:
Article 57(1)(f) of the UK GDPR requires the supervisory authority (the ICO in the UK) to handle complaints lodged by a data subject, investigate the subject matter of the complaint, and inform the complainant of the progress and the outcome of the investigation. It also requires the supervisory authority to cooperate with other supervisory authorities if the complaint involves cross-border processing. However, it does not require the supervisory authority to mediate between the complainant and the controller or processor against which the complaint has been lodged, to resolve the complaint. This is not a task of the supervisory authority under the UK GDPR, although it may be possible in some cases as a way of achieving an amicable solution.Reference:
Article 57(1)(f) of the UK GDPR1
ICO and complaints2

QUESTION 7
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?

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

Correct Answer: A
Section:
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 8
If a complainant disagrees with the decision of the UK's supervisory authority, how do they appeal this decision?

A. To the First Tier Tribunal (Information Rights)
B. To the Information Commissioner
C. To the European Data Protection Supervisor.
D. To the European Commission

Correct Answer: A
Section:
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 to the Upper Tribunal on a point of law, with the permission of the First Tier Tribunal or the Upper Tribunal.Reference:
Information rights and data protection: appeal against the Information Commissioner1
Notice of appeal form2
First Tier Tribunal (Information Rights) website3

QUESTION 9
Who is entitled to a private life by law in the UK?

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

Correct Answer: A
Section:
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 10
When were data protection rights first introduced into UK law'?

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

Correct Answer: C
Section:
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 11
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

A. Belgium
B. France
C. Germany

D. Poland

Correct Answer: C
Section:
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

QUESTION 12
Under which circumstances can the 'domestic purposes' exemption be used to justify non-compliance with the Data Protection Act 2018?
A) An individual sells make up products for commission and uses social media to promote products to friends and family
B) A couple are planning their daughter's wedding and use excel to store contact details and dietary needs of the guests
C) An individual employs a babysitter and stores her bank details in an encrypted document in order to make payments
D) A pansh council keeps a spreadsheet to manage bookings of the village hall, it contains only contact information and time slots
E) A group of students are arranging a house party and using social media to invite people that they do and do not know

A. A, B, C, and E.
B. B. C. D, and E
C. B, and C
D. A. B.C. and D

Correct Answer: C
Section:
Explanation:
The domestic purposes exemption applies to personal data processed by an individual only for the purposes of their personal, family or household affairs. This means that the processing has no connection to any professional or commercial activity. Examples of such processing include writing to friends and family, taking pictures for personal enjoyment, or keeping an address book. However, the exemption does not apply if the individual processes personal data outside the reasonable expectations of the data subject, or if the processing causes unwarranted harm to the data subject's interests. Therefore, the exemption can be used to justify non-compliance with the Data Protection Act 2018 in scenarios B and C, where the processing is purely personal and does not affect the rights and freedoms of others. However, the exemption cannot be used in scenarios A, D and E, where the processing has a professional or commercial element, or involves sharing personal data with third parties without consent or legitimate interest.Reference:
Data Protection Act 2018, Schedule 2, Part 1, Paragraph 21
ICO Guide to Data Protection, Domestic Purposes2
ICO Guide to Data Protection, Exemptions3

QUESTION 13
What is the meaning of storage limitation in relation to UK GDPR Article 5 (1)(e)?

A. Keeping identifiable personal data for no longer than is necessary for the intended processing
B. Storing data in a secure format only permitting access to those with a business need
C. Only storing data in locations within the EU. except where there is an adequacy decision.
D. Limiting the number of records stored in any single repository to minimise risk surface.

Correct Answer: A
Section:
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 for archiving 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.Reference:
UK GDPR, Article 5 (1) (e) and (2)4
UK GDPR, Article 175
UK GDPR, Article 896
ICO Guide to Data Protection, Storage Limitation7

QUESTION 14
Which of the below would be the BEST example of processing that could utilise the Public Interest Task lawful basis?

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

Correct Answer: C
Section:
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 15
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:

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

Correct Answer: B
Section:

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

QUESTION 16
What is the basis of the accountability and data governance obligation (Article 5 (2) of the GDPR)?

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

Correct Answer: B
Section:
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 17
Of the following options which is NOT a purpose of carrying out a Data Protection Impact Assessment (DPIA)?

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

Correct Answer: A
Section:
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 18
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?

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.

Correct Answer: D
Section:
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 19
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

A. B, C. and D
B. A, C, and E
C. A. C, D, and E
D. A, C, and D

Correct Answer: D
Section:
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 20
A privacy notice MUST NOT contain

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

Correct Answer: C
Section:
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 21
What factors should be considered when looking at security of processing under Article 32 of the GDPR?
Select the INCORRECT answer

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

Correct Answer: A
Section:
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 22
Which of the following is NOT a processor obligation?

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

Correct Answer: C
Section:
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 23
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'?

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

Correct Answer: D
Section:
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 24
Describe the act of processing under the authority of a controller or processor as stipulated in UK GDPR Article 29.

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.

Correct Answer: B
Section:
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 25
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?

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.

Correct Answer: A
Section:
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 26
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?

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

Correct Answer: B
Section:

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