NB: If you are reading this as a printed document you are requested to check to ensure that it is the latest version before following the guidance it contains. If you discover this version is out of date, please destroy it and use the latest version.

Document Control Information

Document Name	Sample Paper – Data Protection Practitioner
Purpose of Document	Sample Paper
Document Version Number	9.2
Document Status	Pre-live
Document Owner	Product Development
Data Classification	Restricted - External
Security Category	Low
Prepared By	Product Development
Date of First Draft	07/07/2021
Date Approved	
Approved By	
Next Scheduled Review Date	

Version History

Version Number	Date Amended	Changes Made	Checked By
1.0	09/06/2020	Sample Paper Created	Sophie Spann
9.2	07/07/2021	Sample paper updated based on the changes to the syllabus.	Clare Dye

BCS Practitioner Certificate in Data Protection

Sample Paper

Record your surname / last / family name and initials on the answer sheet.

Sample paper only 40 multiple-choice questions – 1 mark awarded to each question. Mark only one answer to each question. There are no trick questions.

A number of possible answers are given for each question, indicated by either **A. B. C. or D**. Your answers should be clearly indicated on the answer sheet.

Pass mark is [26/40]

This professional certification is not regulated by the following United Kingdom Regulators - Ofqual, Qualifications in Wales, CCEA or SQA

1 Which of the following is **NOT LIKELY** to infringe on a person's right to respect for a private and family life under Article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR)?

A Correspondence being intercepted by a private detective.
B Press publishing photographs of a person at a private wedding with no prior consent.
C Voicemails being listened to by journalists without consent.
D A sports professional being shown on TV performing at a tournament.

2 Which of the following statements are CORRECT regarding the effect of the UK's exit from the EU ("Brexit") on data protection law in the UK:

A. The UK is no longer bound by EU GDPR.
B. The UK is bound by US federal privacy laws.
C. The UK no longer has a data protection law.
D. The UK has been granted adequacy status by the European Commission.

A A & D
B A, C & D
C B & D
D A, B, C & D

3 When is a company **NOT** required to comply with the EU GDPR?

A It is based inside the EU but does not send direct marketing to its customers.
B It is based outside the EU and does not target customers within the EEA.
C It is based in the EU but does not store personal data.
D It targets customers globally and has clear terms of service.

4 Which of the following definitions applies to Pseudonymisation?

A The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.
B Information which does not relate to an identified or identifiable natural person or to personal data.
C In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data by automated means.
D Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person.

5 Which of the following statements **BEST** describes the requirement for maintaining accuracy (Article 5(1)(d))?

A Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
B Third parties opinions regarding a data subject should never be recorded as they are objective and may be inaccurate.
C If a company takes action against a customer for non-payment that was later found to be an error on the company's part, no record of the error should be kept on the customers file.
D A company must accurately record the source of personal data as well as taking every reasonable step to ensure incorrect data are rectified or erased without delay.

6 What is the **MOST LIKELY** lawful basis for the following processing:

A company has sold tickets to an event and want to contact customers to inform them of a change in the timing of the event.

A Consent.
B Legitimate Interests.
C Contract.
D Public Interest Task.

7 Under the Data Protection Act 2018, which of these does **NOT** give a specific basis in UK law for relying on specific Article 9 conditions?

A Public task.
B Archiving, research or statistics.
C Public health.
D Social security and social protection.

8 Identify the accountability and data governance obligation.

A Controllers are responsible for ensuring compliance in all processing activities carried out by themselves and their third party processors.
B Controllers are responsible for their own processing activities only.
C Third party processors act only on the instructions of controllers and have no accountability for the compliance of that processing.
D All processors and controllers have equal accountability for their own, and each other's compliance.

9 In which circumstance would a DPIA **NOT** be appropriate?

A Planning the implementation of a new database.
B Determining if a dedicated DPO is required.
C Reviewing a proposed new SMS marketing strategy.
D Considering changes to security controls applied to personal data.

10 Which of the following is **NOT** a key part of every Data Protection Impact Assessment (DPIA)?

A Report outcome to the ICO.
B Assess necessity and proportionality.
C Sign off and record outcomes.
D Identify the need for a DPIA.

11 Which of the following **BEST** describes the requirements for records of processing?

A Organisations with 250 or more employees must document all their processing activities.
B Information collected during one-off recruitment campaigns does not need to be recorded if it is not to be stored long term.
C Organisations using the Vital Interests lawful basis are exempt from this requirement.
D Organisations with a Data Protection Officer must document all their processing activities.

12 Which of the following is **NOT** always required in a privacy notice?

A Details of security controls applied to personal data.
B The right to lodge a complaint with a supervisory authority.
C The retention periods for the personal data.
D Contact details for the DPO if there is one.

13 Which of the following is **NOT** a way to adopt a data protection by design and by default approach?

A Carry out regular Legitimate Interest Assessments.
B Consider the implications of data protection as part of all new system integrations.
C Offer strong privacy defaults and user friendly documentation and controls.
D Make data protection an essential component of the core functionality of your processing systems and services.

14 Which of the following statements is INCORRECT in regards to the security requirement of Article 32 of the GDPR?

A Companies should always employ state of the art security controls to all personal information.
B Companies must make data protection an essential component of the core functionality of your processing systems and services.
C Security controls must effectively protect the confidentiality, integrity and availability of personal data.
D A balanced approach should be taken using frequent risk analysis.

15 Which of the following statements is CORRECT?

A A DPO must report directly to the highest level of management.
B A DPO is solely responsible for a company's compliance with data protection laws.
C A DPO must ensure that compliance does not undermine other business objectives.
D Companies may appoint multiple DPOs where the processing is large-scale.

16 A third party company provides a marketing service to your customers. The third party sends unconsented third party marketing content to your customers via email, following instructions from your marketing team.

In the event of a complaint to the ICO, what is the position on accountability?

A Both companies have acted unlawfully and are accountable.
B The controller is solely accountable for the breach as the processor was acting on their instruction.
C The processor is solely responsible as they sent the mails.
D Providing a suitable LIA and a DPIA are completed there is no possibility of a complaint being upheld.

17 A travel agency has designed a booking system in collaboration with an airline and two hotel chains. Each of the companies is able to enter and view customer bookings. The travel agency commissioned and paid for the system to be built. The companies have clear documentation outlining responsibilities and they have equal input in determining the way the data is collected, stored and processed.

Select the option that accurately describes the controller processor relationship that applies in this scenario:

A The travel agency is the controller, the airline and hotel chains are processors.
B All parties are joint processors, each having liability only for their specific actions.
C All parties are joint controllers and are accountable for ensuring compliance is maintained.
D The airline is the controller as it is required to process sensitive PII, the travel agency and hotel chain are processors.

18 You have been asked to review data processing agreements between EG Accounts Ltd, a company providing accounting and payroll services for construction companies and their customer; LPJ Building Ltd.

You are preparing a list of facts to assist in creating the agreement.

Which of the following statements is INCORRECT?

A EG Accounts Ltd must only process employee data according to explicit instructions from LPJ Building Ltd.
B The processing agreement should clearly state what happens to the data when the contract is ended.
C LPJ Building has no liability for the way EG Accounts Ltd processes and stores the data.
D In the event of a serious data breach, both companies may be investigated by the ICO.

19 What does the following definition describe?

"A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data".

A An asset owner.
B A third party.
C An ISA.
D A recipient.

20 Which of the following countries does **NOT** have an EU Commission adequacy decision allowing restricted transfers?

A Australia.
B Uruguay.
C Japan.
D Andorra.

21 Under what circumstances is the right to object (GDPR Article 12) an absolute right?

A Where the data are being processed for direct marketing.
B When the data involved includes special category data.
C Where the data is being processed by religious organisations.
D When the data includes medical records.

22 Article 23 allows member states to restrict the scope of the obligations and rights provided for in articles 12 - 22 by way of legislation.

How has the UK made use of this?

A The DPA 2018 permits a data controller to disclose personal data for the prevention or detection of crime or for the apprehension and prosecution of offenders.
B Under the existing Computer Misuse Act 1990 article 23 permits a controller to disclose PII to authorities for the prevention or detection of crime.
C The UK has not made any legislation relating to GDPR restrictions.
D The Freedom of Information Act 2000 requires controllers to release PII when it is deemed to be in the public interest.

23 What are some of the mandatory factors of Independent Supervisory Authorities?

A Each supervisory authority may be subject to financial penalties from their respective governments if they fail to meet their financial targets.
B They must be entirely independent bodies, competent, and they must provide other ISAs with mutual assistance.
C They must have full jurisdiction over all data protection matters and they must be fully independent.
D Supervisory authorities must be granted powers of investigation and arrest, and they must be given sufficient and independent funding by the state.

24 A German data subject feels their privacy rights under Article 21 of the GDPR have been breached by an international social media company. The company has a data protection representative based in Spain. The data subject submitted a DSR to the company but feels it has not been correctly addressed.

To whom should the data subject escalate their concern?

A Either a German ISA, or the Spanish Data Protection Agency (AEPD).
B Only the Spanish Data Protection Agency (AEPD).
C Only the German ISA.
D The European Data Protection Board (EDPB).

25 Which of the following is **NOT** a role of the EDPB?

A Provide general guidance to clarify the law.
B Advise the European Commission on issues related to the protection of personal data.
C Adopt consistency findings in cross-border data protection cases.
D Supervise the Independent Supervisory Authority's handling of major cases.

26 Under which circumstances is it **MOST LIKELY** that the ICO would impose a higher tier fine (up to £17.5 million or 4% global turnover)?

A Failure to obtain proper consent or soft opt-in before contacting customers for marketing purposes.
B Failure to appoint a Data Protection Officer where one is required.
C Failure to notify customers of a significant compromise of their data.
D Failure to implement state of the art security controls to protect all personal data.

27 You are working in the data protection team of a large company holding multiple databases containing personal data. Your team is responsible for handling personal data breaches.

You are asked to look at the following cases, which of these does **NOT** constitute a personal data breach?

A Emails sent to customers that have not provided correct consent.
B Customer credit card data being illicitly photographed by an employee.
C Paper copies of customer postal addresses lost on public transport.
D Emails sent to customers accidentally containing other customers' email addresses.

28 You are a DPO for a supermarket chain. The IT department have alerted you to a potential data breach involving an old marketing database. You have been asked to oversee the investigation and determine if the ICO and data subjects should be informed.

How do you determine if the ICO and the data subjects should be notified?

A If any database containing personal data has been accessed by an unauthorised person.
B If any personal information has been made publicly available, for example on the internet.
C Only if the breach is likely to result in a significant risk to the data subjects rights and freedoms.
D If the data subjects are existing customers.

29 What is the proper course of action for a data protection complaint?

A A data subject makes a complaint to the ICO, the ICO then raises an information notice with the controller instructing them to process the complaint accordingly.
B A data subject must log a complaint first with the DPO at a company, who may escalate to the ICO.
C A data subject may make a complaint to the ICO after having first submitted a Data Subject Access Request to the company they wish to complain about.
D A data subject may make a complaint directly to the ICO who are bound to investigate the matter to a suitable extent.

30 In which of the following circumstances may the judicial courts deal with data protection matters?

A Appealing a decision of a supervisory authority.
B Issuing enforcement notices.
C Imposing fines following breaches of compliance.
D Ordering searches of company premises.

31 What is the Age Appropriate Design Code?

A A data protection code of practice for online services likely to be accessed by children.
B A code of practice for ensuring parental consent is in place when processing data of children under 13.
C A regulation that sits alongside the GDPR mandating enhanced security controls for children's data.
D A framework for developers advising on secure coding for apps likely to be used by children.

32 Which of the following is an exempt public authority or public body according to section 7 of the DPA 18?

A Public Health England.
B A community council in Wales.
C The Passport Office.
D The National Centre for Cyber Security (NCSC).

33 Other than when specifically exempt under section 7 of the DPA, when are public authorities required to appoint a DPO?

A Under all circumstances.
B Always, except if they are a court acting in their judicial capacity.
C When they employ over 250 employees or conduct large scale processing of personal data.
D Only if they conduct large scale processing of personal data, or profiling.

34 Select the **FALSE** statement regarding the restriction for health data in the right of access:

A It restricts companies from disclosing health data in response to a subject access request in certain circumstances.
B It does not apply to health professionals.
C It does not apply if the information is already known by the data subject.
D It restricts data subjects from making data subject requests regarding health care data.

35 What is the primary area of data protection that PECR cover?

A All forms of electronic communication.
B All forms of marketing.
C Websites and cookies.
D Postal marketing.

36 What is the current status of PECR?

A PECR were implemented in 2005. They have since been superseded by the GDPR and the DPA 2018.
B PECR implement the ePrivacy Directive. They sit alongside the DPA 2018 and are due to be replaced by the upcoming ePrivacy Regulation.
C PECR were the original privacy regulations on which the DPA 1998 was based. It has now been replaced by the ePrivacy Directive.
D PECR are based upon the ePrivacy Regulation and came into force in 2018 alongside the GDPR.

37 What is the purpose of the Employment Practices Code?

A It mandates further restrictions on how you may process employee information.
B It provides additional lawful bases for processing data in relation to employment.
C It gives recommendations on how to meet the legal requirements of data protection legislation when employing staff.
D It delivers guidance on employing a suitable Data Protection Officer.

38 Describe how the use of CCTV is governed by data protection law:

A CCTV is subject to the DPA 2018.
B CCTV is exempt from GDPR under the law enforcement exemption.
C CCTV is not covered by the DPA but is subject to the Freedom of Information Act.
D CCTV does not constitute personal data and therefore is not covered by data protection legislation.

39 You are working as a DPO for a travel company. The marketing team would like to use cookies on the company website to track user activity.

Which privacy legislation applies?

A None; the ePrivacy regulation is still in draft.
B Both GDPR and PECR apply.
C Only PECR applies to cookies.
D GDPR has now superseded PECR which no longer applies.

40 How are data sharing practices governed by data protection law?

A Data sharing practices are covered in the DPA 2018, there is a statutory Code of Practice that provides specific guidance.
B Data sharing practices are still subject to the DPA 1998 until the new statutory Code of Practice is published.
C Data sharing practices are covered by the PECR.
D Data sharing practices are governed by the Freedom of Information Act.

End of Paper

Question	Answer	Syllabus Sections	Rationale
1	**D**	LO1.1.	One cannot reasonably expect privacy when performing in a public event
2	**A**	LO1.2.	All of these are current, none have been superseded.
3	**B**	LO1.3.	See article 3, GDPR.
4	**A**	LO2.1.	See article 4 (5), GDPR.
5	**D**	LO2.2.	See Article 5(1)(d), GDPR.
6	**C**	LO3.1.	See article 6, GDPR.
7	**A**	LO3.2.	See article 9, GDPR.
8	**A**	LO4.1.	See Article 5 (2), GDPR.
9	**B**	LO4.2.	See Article 35, GDPR.
10	**A**	LO4.3.	See Article 35, GDPR.
11	**A**	LO4.4.	See Article 30, GDPR.
12	**A**	LO4.5.	See Article 13, 14, GDPR.
13	**A**	LO4.6.	See Article 25, GDPR.
14	**A**	LO4.7.	See Article 32, GDPR.
15	**A**	LO4.8.	See Article 37-39, GDPR.
16	**A**	LO5.1.	See Article 24 & 28, GDPR.
17	**C**	LO5.2.	See Article 26, GDPR.
18	**C**	LO5.3.	See Article 29, GDPR.
19	**B**	LO5.5.	See Article 4 (10), GDPR.
20	**A**	LO6.1.	A current list of countries granted adequacy decisions is published on the European Commission Data Protection website.
21	**A**	LO7.1.	See Article 12, GDPR.
22	**A**	LO7.3.	See DPA 18 Schedule 2.
23	**B**	LO8.1.	See Article 52, GDPR.

Question	Answer	Syllabus Sections	Rationale
24	**A**	LO8.2.	See Article 58, GDPR.
25	**D**	LO8.3.	See Articles 64, 65 & 70, GDPR.
26	**A**	LO9.4.	See Articles 83 & 84, GDPR.
27	**A**	LO9.1.	See Article 4 (12) GDPR.
28	**C**	LO9.2.	See Articles 33 & 34, GDPR.
29	**D**	LO9.3.	See Article 57 (1)(f), GDPR.
30	**A**	LO9.6.	See Article 78, GDPR.
31	**A**	LO10.1.	See DPA 18 section 123.
32	**B**	LO11.1.	See DPA 18 section 7.
33	**B**	LO11.2.	See DPA 18 section 7.
34	**D**	LO11.3.	See DPA 18 schedule 3.
35	**A**	LO12.1.	See PECR 2003.
36	**B**	LO12.2.	The ePrivacy Regulation was due to come in to force alongside GDPR in 2018 but it is yet to be agreed.
37	**C**	LO13.1.	See the Employment Practices Code.
38	**A**	LO13.2.	CCTV constitutes personal data and is therefore in scope of the DPA 18.
39	**B**	LO13.3.	Cookies that process personal data are subject to the same regulations as other processing activities.
40	**A**	LO13.4.	Data sharing practices are subject to the data protection act, the requirements of which will be clarified in the upcoming code of practice.