BCS Practitioner Certificate in Data Protection v9.9

Sample Paper

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

Sample paper consists of 40 multiple choice questions.

Multiple choice questions allow only one correct answer to be selected for 1 mark.

1 mark awarded 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: 26/40
Time allowed: 90 minutes

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

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 (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 (European Union) EU ("Brexit") on data protection law in the UK?

A. The UK is no longer bound by the 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 and D only.
B A, C and D only.
C B and D only.
D A, B, C and D.

3 When is a company **not** required to comply with the European Union (EU) GDPR?

A When it is based inside the EU but does not send direct marketing to its customers.
B When it is based outside the EU and does not process personal data of customers within the European Economic Area (EEA).
C When it is based in the EU but does not store personal data.
D When it targets customers globally and has clear terms of service.

4 Which of the following **correctly** defines pseudonymisation?

A The processing of personal data in such a manner that it can no longer be attributed to a specific data subject, without the use of additional information.
B Information that does not relate to an identified or identifiable natural person, or to personal data.
C Any operation, or set of operations, that 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 customer's file.
D A company should precisely record the source of personal data as well as taking every reasonable step to ensure incorrect data are rectified or erased without delay.

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

What is the **most likely** lawful basis for this processing?

A Consent.
B Legitimate interests.
C Contract.
D Public interest task.

7 You are the newly appointed Data Protection Officer (DPO) for an innovative marketing company. The company has developed a new product that will be installed in shopping centres. A digital screen is placed at the entrance of the centre. A camera scans the customers as they enter the building, and an Artificial Intelligence (AI) solution analyses the footage in real-time. The footage is stored and used to further train the AI solution.

The AI solution identifies customers meeting certain criteria and presents bespoke advertisements based on their profile. For example, if a customer using a wheelchair enters, the screen will display an advertisement for a mobility retail store.

The screen will be accompanied by a privacy notice at the entrance of the centre, which explains the technology and informs customers that they should not enter if they do not wish to be recorded.

The previous DPO advised the company that this will involve the processing of special category data and the company can rely on the Article 9 condition of "manifestly made public" by the data subject. You have been asked to assess this advice and make a recommendation to the company.

Which of the following statements is **most** appropriate in respect of the previous DPO's advice to the company.

A The previous DPO was incorrect because the solution is not processing special category data.
B The previous DPO was incorrect because the "manifestly made public" condition requires the data subjects to have made a deliberate effort to make the information public.
C The previous DPO was correct because the information will be in the public domain and available to anyone who observes the data subject.
D The previous DPO was correct because the data subjects have made a choice to allow themselves to be recorded.

8 Which of the following **correctly** describes the accountability and data governance obligation?

A Controllers are responsible for ensuring compliance in all processing activities carried out by themselves and any processors they appoint.
B Controllers are responsible for their own processing activities only.
C 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 of the following circumstances would a Data Protection Impact Assessment (DPIA) **not** be appropriate?

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

10 Which of the following statements relating to the benefits of Artificial Intelligence (AI) is **incorrect**?

A The benefits of AI systems always outweigh the risks.
B AI systems can bring about more efficiency in repetitive tasks, thereby reducing costs.
C AI systems can quickly spot patterns in large datasets that would take humans many years.
D The benefits of AI systems are not always worth the associated risks.

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 (DPO) must document all their processing activities.

12 RecruitMe is an online recruiting platform. They are developing an Artificial Intelligence (AI) system which helps them to filter applications to popular jobs, and automatically reject applicants that do not meet the required level. The project manager decides that a Data Protection Impact Assessment (DPIA) will be required prior to deploying this new AI system. As part of this DPIA, RecruitMe want to consult with relevant stakeholders.

Which of the following stakeholders would it be appropriate for RecruitMe to consult with?

A. Previous or current job applicants that used RecruitMe's platform.
B. People with lived experience of automatic application rejection.
C. Independent AI experts.
D. RecruitMe's Data Protection Officer (DPO).

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

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 regarding the security requirement of Article 32 of the GDPR is **incorrect**?

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

15 Which of the following statements regarding Data Protection Officers (DPOs) is **correct**?

A A DPO must ensure that compliance does not undermine other business objectives.
B A DPO is solely responsible for a company's compliance with data protection laws.
C A DPO must report directly to the highest level of management.
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 marketing content to your customers via email, following instructions from your marketing team.

In the event of a complaint to the Information Commissioner's Office (ICO), which of the following **correctly** describes 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 Provided a suitable legitimate interests assessment and a Data Protection Impact Assessment (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.

Which of the following correctly describes the controller/processor relationship that applies in this scenario?

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

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 has 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 Information Commissioner's Office (ICO).

19 Which of the following stipulations is **not** specifically required in a contract between a controller and a processor?

A That the processor deletes or returns the personal data at the end of the services.
B That the processor makes available all information necessary to demonstrate compliance with the GDPR.
C That the processor ensures all personnel involved in the processing respect the confidentiality.
D That the processor conducts and provides a Data Protection Impact Assessment (DPIA).

20 Under the UK data protection regime, which of the following office-holders is able to declare a third country as providing an adequate level of protection for personal data?

A The Information Commissioner.
B The Secretary of State for Science, Innovation and Technology.
C The Prime Minister.
D The Secretary of State for Foreign Affairs.

21 Under which of the following circumstances is the right to object (GDPR Article 21) an absolute right?

A Where the data is 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 GDPR 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 Data Protection Act 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 personal data to authorities for the prevention or detection of crime.
C The UK has not made any legislation relating to GDPR Article 23 restrictions.
D The Freedom of Information Act (FoIA) 2000 requires controllers to release personal data when it is deemed to be in the public interest.

23 Which of the following is one of the mandatory factors of Independent Supervisory Authorities (ISAs)?

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, be 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 They 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 data subject access request to the company, but feels it has not been correctly addressed.

To which of the following would you advise the data subject to escalate their concern?

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

25 Which of the following is **not** a role of the European Data Protection Board?

A Providing general guidance to clarify the law.
B Advising the European Commission on issues related to the protection of personal data.
C Adopting consistency findings in cross-border data protection cases.
D Supervising the Independent Supervisory Authorities' (ISA) handling of major cases.

26 Under which of the following circumstances is it **most likely** that the Information Commissioner's Office (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 (DPO) 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 the following does **not** constitute a personal data breach?

A Paper copies of customer postal addresses lost on public transport.
B Customer credit card data being illicitly photographed by an employee.
C Unconsented emails sent to customers.
D Emails sent to customers accidentally containing other customers' email addresses.

28 You are a Data Protection Officer (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 Information Commissioner's Office (ICO) and data subjects should be informed.

Which of the following **correctly** describes how you **should** 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 Under the statutory complaint framework introduced by the Data (Use and Access) Act, which of the following describes the proper course of action when a data subject makes a complaint directly to a controller?

A The controller must immediately escalate the complaint to the Information Commission.
B The controller must resolve the complaint and pay compensation within 72 hours.
C The controller must acknowledge receipt of the complaint within 30 days and respond to it without undue delay.
D The controller has 40 working days to either accept or reject the complaint.

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

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

31 Which of the following **correctly** describes the ICO Children's 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, maintaining enhanced security controls for children's data.
D A framework for developers, advising on secure coding for applications 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 Data Protection Act 2018?

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

33 Other than when specifically exempt under section 7 of the Data Protection Act, which of the following **correctly** describes when public authorities are required to appoint a Data Protection Officer (DPO)?

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

34 Which of the following statements regarding the restriction for health data in the right of access is **incorrect**?

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

35 What is the primary area of data protection that the Privacy and Electronic Communications Regulations (PECR) 2003 cover?

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

36 Which of the following areas are **not** covered by the Privacy and Electronic Communications Regulations (PECR) 2023?

A Email marketing.
B Cookies and similar technologies.
C Postal marketing.
D Withholding telephone numbers.

37 Which of the following is **not** best practice when collecting and keeping employment records?

A Asking workers to regularly check their personal information to make sure it is accurate and up to date.
B Ensuring employees can access each other's occupational health records so they can provide appropriate support.
C Reminding workers of where to find up to date privacy information outlining how their data is processed.
D Identifying a lawful basis for collecting and using workers' personal information.

38 Which of the following **correctly** describes how the use of Closed-Circuit Television (CCTV) is governed by data protection law?

A CCTV is subject to the Data Protection Act 2018.
B CCTV is exempt from GDPR under the law enforcement exemption.
C CCTV is not covered by the Data Protection Act, 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 Data Protection Officer (DPO) for a travel company. The marketing team would like to use cookies on the company website to track user activity.

Which of the following 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 Which of the following correctly describes how data sharing practices are governed by data protection law?

A Data sharing practices are covered in the Data Protection Act 2018, where there is a statutory Code of Practice that provides specific guidance.
B Data sharing practices are still subject to the Data Protection Act 1998, until the new statutory Code of Practice is published.
C Data sharing practices are covered by the Privacy and Electronic Communications Regulations (PECR) 2003.
D Data sharing practices are governed by the Freedom of Information Act (FoIA).

End of Paper

Question	Answer	Rationale	Syllabus Sections
1	**D**	One cannot reasonably expect privacy when performing in a public event.	LO1.1
2	**A**	Both of these are statements are current and correct.	LO1.2
3	**B**	See Article 3, EU GDPR.	LO1.3
4	**A**	See Article 4 (5), UK GDPR.	LO2.1
5	**D**	See Article 5(1)(d), UK GDPR.	LO2.2
6	**C**	See Article 6, UK GDPR.	LO3.1
7	**B**	See ICO guidance on "Manifestly Made Public" condition.	LO3.2
8	**A**	See Article 5 (2), UK GDPR.	LO4.1
9	**B**	See Article 35, UK GDPR.	LO4.2
10	**A**	See the latest ICO guidance on AI and data protection.	LO14.1
11	**A**	See Article 30, UK GDPR.	LO4.4
12	**D**	See the latest ICO guidance on AI and data protection.	LO14.2
13	**A**	See Article 25, UK GDPR.	LO4.6
14	**C**	See Article 32, UK GDPR.	LO4.7
15	**C**	See Articles 37-39, UK GDPR.	LO4.8
16	**A**	See Articles 24 and 28, UK GDPR.	LO5.1
17	**D**	See Article 26, UK GDPR.	LO5.2
18	**C**	See Article 29, UK GDPR.	LO5.3
19	**D**	See Article 28(3) of the UK & EU GDPR.	LO5.4
20	**B**	See Section 17A of the amended Data Protection Act 2018.	LO6.1
21	**A**	See Article 21(2), UK GDPR.	LO7.1
22	**A**	See Data Protection Act 2018 Schedule 2.	LO7.3
23	**B**	See Article 52, EU GDPR.	LO8.1

24	**D**	See Article 58, EU GDPR.	LO8.1
25	**D**	See Articles 64, 65 and 70, EU GDPR.	LO8.1
26	**A**	See Article 83 UK GDPR.	LO9.4
27	**C**	See Article 4 (12) UK GDPR.	LO9.1
28	**C**	See Articles 33 and 34, UK GDPR.	LO9.2
29	**C**	See Article 57 (1)(f), UK GDPR.	LO9.3
30	**B**	See Article 78, UK GDPR.	LO9.6
31	**A**	The ICO Children's Code is a set of standards created by the Information Commissioner's Office to ensure that online services protect children's privacy and data.	LO10.1
32	**B**	See Data Protection Act 2018 section 7.	LO11.1
33	**C**	See Data Protection Act 2018 18 section 7.	LO11.2
34	**A**	See Data Protection Act 2018 18 schedule 3.	LO11.3
35	**D**	See Privacy and Electronic Communications Regulations (PECR) 2003.	LO12.1
36	**C**	See Privacy and Electronic Communications Regulations (PECR) 2003. (scope).	LO12.1
37	**B**	Allow employees to access another employee's sensitive personal data is a direct contravention of GDPR principles.	LO13.1
38	**A**	CCTV constitutes personal data and is therefore in scope of the Data Protection Act 2018.	LO13.2
39	**B**	Cookies that process personal data are subject to the same regulations as other processing activities.	LO13.3
40	**A**	Data sharing practices are subject to the data protection act, the requirements of which will be clarified in the upcoming code of practice.	LO13.4