

BCS Certificate in Data Protection

Specimen Paper – This is not a complete sample paper

(Marking Guidelines appear after the exam paper)

Section A – multiple-choice questions

Answer all of the 20 questions – each answer carries 1 mark

Section B – short answer questions

Answer all of the 8 questions – each answer carries 5 marks

Section C – essay questions

Answer 4 questions from 6 – each answer carries 10 marks

Pass Mark: 50%

Distinction Mark: 80%

NOTE: All of the organisations and individuals mentioned in questions on this paper are entirely fictional and no reference to any real organisation or person is intended or implied.

Copying of this paper is expressly forbidden without the direct approval of BCS, The Chartered Institute for IT.



This page is intentionally blank.

Section A

Multiple-choice answers – 1 mark each

Answer all 20 questions (Please use EDPAC sheet provided for answers)

NOTE: Choose only one answer per question

- 1 Which of the following is a data subject?
- A Martin Luther King.
 - B The BBC.
 - C Tony Blair.
 - D Homer Simpson.
- 2 What is the minimum age for subject access in England and Wales?
- A 11.
 - B 16.
 - C 21.
 - D None of the above.
- 3 Which of the following is a disclosure?
- A A pharmacist telling her neighbour about a prescription she gave the local vicar.
 - B A bank statement found in the street.
 - C Both.
 - D Neither.
- 4 An employee of the data controller is:
- A A third party.
 - B A data processor.
 - C A recipient.
 - D None of the above.

- 5 A Monetary Penalty Notice served by the Information Commissioner can impose a maximum fine of:
- A £5000.
 - B £500,000.
 - C Unlimited fine.
 - D £500.
- 6 When should you conduct a Privacy Impact Assessment?
- A Before a project has been designed or in the early stages of design.
 - B Once the project has been implemented.
 - C One to two years after the project is underway when privacy issues have become clearer.
 - D It makes no difference.

Questions 7-20 consist of similar style questions.

Section B

Short 'bullet point' type answers (making 5 distinct points) – 5 marks each

Answer all 8 questions
(Answer booklets provided)

- 1 Under the Data Protection Act 1998, do parents have a right to see information relating to their children when it is held by an organisation? Give reasons for your answer.

[5 Marks]

- 2 In the context of the Data Protection Act 1998, can the police request and expect to receive information from an organisation about a suspect in a burglary? What should an organisation consider under the Act when it receives such a request from the Police?

[5 Marks]

- 3 Under what circumstances can the Information Commissioner serve:

- a) an Information Notice *and*
- b) an Enforcement Notice.

What must be included in such Notices?

[5 Marks]

- 4 A recruitment company has decided to outsource its payroll function to another company. What are the main implications of this decision in terms of Principle 7 of the Data Protection Act 1998?

[5 marks]

Questions 5-8 consist of similar style questions.

Section C

Essay style answers – 10 marks each
Answer 4 of the following 6 questions
(Answer booklets provided)

- 1** A company selling personal life insurance products wants to increase business through marketing both existing and potential new customers by telephone and fax. What are the main implications of this marketing strategy under the Privacy of Electronic Communications (EC Directive) Regulations 2003?

[10 marks]

- 2** The Mixenden Borough Partnership has received money from central government to install a CCTV system in the town centre to help reduce crime and anti-social behaviour in the area. The partnership is made up of many partners such as private businesses as well as the council. They plan to contract out the running of the system to Keep It Safe Limited. Assuming the CCTV system will be capturing personal data, identify key data protection considerations relating to this scenario.

Questions 3-6 consist of similar style questions.

--End of Paper--

Marking Guidelines

Section A

Question No	Answer
1	C
2	D
3	C
4	C
5	B
6	A

Section B

- 1 Under the Data Protection Act 1998, do parents have a right to see information relating to their children when it is held by an organisation? Give reasons for your answer.

[5 Marks]

Marking Guidelines

- Section 7 of the DPA gives a right of access to the data subject and not directly to others. (This right includes a right, in most cases, not just to see the data but also to have a copy of it as well). This means that parents do not have an automatic right to see their children's data under the DPA.
- A parent of a child who is too young to understand the nature of a subject access request can make a request on the child's behalf.
- The data controller would need to satisfy itself that the request was being made by the parent on behalf of the child and ascertain/verify the identity of the parent.
- Where an organisation receives a subject access request in respect of a child they consider is able to understand the nature of the request they should refuse to disclose.
- It is generally accepted that, unless there are indications to the contrary, a child aged 12 or over would generally be expected to understand the nature and consequences of a subject access request. (Gillick competency /Fraser test).

- 2 In the context of the Data Protection Act 1998, can the police request and expect to receive information from an organisation about a suspect in a burglary? What should an organisation consider under the Act when it receives such a request from the Police?

[5 Marks]

Marking Guidelines

- Under the Data Protection Act the Police have no automatic right of access to personal data relating to suspects and a data controller is under no obligation to provide access.
- However, the DPA does allow data controllers to disclose to the Police providing the criteria in the exemption in Section 29(3) can be met:
 - Section 29(3) – provides an exemption from the non-disclosure provisions if
 - Disclosure is for purposes of prevention or detection of crime or the apprehension or prosecution of offenders, and
 - Not disclosing would be likely to prejudice these purposes.
- The “non-disclosure provisions” include Principle 1 (except to the extent to which it requires compliance with Schedules 2 & 3) , and Principle 2
- From a precautionary and procedural perspective, the data controller should require the police request to be made in writing, signed by a senior police officer, specifying the reason for the request and confirming that, in the opinion of the Police, not disclosing the data would prejudice the investigation.

3 Under what circumstances can the Information Commissioner serve:

- c) an Information Notice *and*
- d) an Enforcement Notice.

What must be included in such Notices?

[5 Marks]

Marking Guidelines

Information notice – this can be served when:

- the IC has received a request for assessment under Section 42 of the DPA and requires the information to enable him to carry out the assessment.
- the IC reasonably requires information in order to determine whether a data controller has complied or is complying with the data protection principles

Enforcement Notice – this can be served when:

- the IC is satisfied that the data controller has contravened or is contravening any of the data protection principles and;
- the IC requires the data controller to take some form of remedial action (which could include ceasing particular processing)

Information Notice and Enforcement Notice – both notices must contain:

- information about the right of appeal to the First -tier Tribunal (Information Rights)
- a description of the action required of the data controller
- the timescales (i.e. dates by which action must be undertaken)

- 4 A recruitment company has decided to outsource its payroll function to another company in the UK. What are the main implications of this decision in terms of Principle 7 of the Data Protection Act 1998?

[5 marks]

Marking Guidelines

- The recruitment company is a data controller. The other company is going to be processing personal data on behalf of the recruitment company and will therefore be a data processor.
- Principle 7 requires the recruitment company to choose a processor that provides sufficient guarantees in respect of technical and organisational security measures and take reasonable steps to ensure compliance with those measures.
- Principle 7 also requires the recruitment company to have a contract with the processor which is made or evidenced in writing under which:
 - (i) the processor is only to act upon the instructions of the recruitment company as data controller, and
 - (ii) the processor must comply with obligations which are equivalent to those imposed upon the recruitment company by Principle 7

Section C

- 1 A company selling personal life insurance products wants to increase business through marketing both existing and potential new customers by telephone and fax. What are the main implications of this marketing strategy under the Privacy of Electronic Communications (EC Directive) Regulations 2003?

[10 marks]

Marking Guidelines

- PECR regulates the sending of unsolicited marketing messages via electronic means which includes telephone and fax.
- The regulations treat companies and individuals differently. Sole traders and partnerships are also considered to be individuals.
- **Fax:**
 - It is unlawful to send an unsolicited fax to an individual unless they have consented. As the company plans to market potential new customers which are likely to include individuals it should obtain their consent in advance.
 - The company can fax other companies that have not previously registered with the Fax Preference Service (FPS). There is a cost for checking lists against FPS. Any number found on the FPS must not be contacted unless the company concerned has advised the marketer that they do not object to receiving a marketing fax from them.
- **Telephone:**
 - The company must screen its telephone numbers against the TPS or CTPS and not contact any telephone number appearing in either list, unless the individual / company has previously given an indication of non objection to being contacted by telephone for direct marketing purposes.
 - There is a fee for screening numbers against the TPS.
- **Fax / Telephone:**
 - The company should record on an internal suppression list the details of any person who objects to being contacted, so that they cannot be telephoned again in the future.
 - When embarking on its telephone marketing campaign, the company representative must state the company's name and if so requested, the address or telephone number they can ring to object. Faxes should also include contact details.
 - Automated Telephone Campaigns: i.e. those which operate without human intervention, are unlawful unless the recipient individual or company has previously notified the caller that they consent to receiving such communications.
 - PECR is enforced by the ICO using similar powers of enforcements to those under the DPA.
 - Those seeking legal remedies have the right to seek redress through the courts if they have suffered damage as a result of a breach of the



Regulations.

- 2 The Mixenden Borough Partnership has received money from central government to install a CCTV system in the town centre to help reduce crime and anti-social behaviour in the area. The partnership is made up of many partners such as private businesses as well as the council. They plan to contract out the running of the system to Keep It Safe Limited. Assuming the CCTV system will be capturing personal data, identify key data protection considerations relating to this scenario. **[10 marks]**

Marking Guidelines

- Who is the data controller? Each of the partners will be a separate legal entity (i.e. a data controller) in its own right, with separate liability for compliance with the Act **(2 marks)**
- Notification to the ICO is required for those data controllers using CCTV systems

(No more than 3 marks to be awarded for this section)

- Key points below, as contained in the ICO's CCTV code of practice:
 - cameras have been sited so that their images are clear enough to allow the police to use them to investigate a crime
 - there are visible signs showing that a CCTV system is in operation and the controllers contact details are displayed on the sign where it is not obvious who is responsible for the system
 - the recorded CCTV images are securely stored, where only a limited number of authorised persons may have access to them
 - the recorded images will only be retained long enough for any incidents to come to light (e.g. for a theft to be noticed)
 - recordings will only be made available to law enforcement agencies involved in the prevention and detection of crime, and no other third parties
 - the operating equipment is regularly checked to ensure that it is working properly
 - the controller knows how to respond to subject access requests for images

(No more than 5 marks to be awarded for this section)

- There must be a contract in place with Keep It Safe Limited. Consider who will enter into the contract with Keep It Safe Ltd (all the partners or just one of them?)
- Keep It Safe Ltd will be a data processor. Need a processing contract. There must be clauses in the contract that:
 - Keep It Safe Ltd will only act on the instructions of the partners (maybe one of them has been nominated to act on behalf of the others)
 - it will take reasonable steps to ensure security of the personal data and also the reliability of its employees
 - give the controller the right to check Keep It Safe's compliance with the security measures specified in the contract, such as a right to audit processing.



(No more than 2 marks to be awarded for this section)