BCS Foundation Certificate in Data Protection v3.9

Exercise booklet

Contents

Document version history

Document version	Changes made
1.0 April 2026	Document created

Exercise 1

List all the relevant instruments, conventions, laws, and declarations that apply to protecting the right to privacy, in chronological order, and specify which of these are binding, and whether they apply globally, in Europe, or just the UK.

Exercise 2

In which of the following scenarios might the GDPR (either EU or UK) apply? In each case, say which of the provisions of Article 3 apply.

1. A resident of Poland applying for a driving licence in Poland

2. A company based in Italy selling goods primarily to South Africa

3. A German company using a US-based HR system provided by its parent company

4. An Indian national visiting a Spanish website

5. A resident of Egypt ordering products from a company based in Finland

6. A multinational company based in Singapore with offices in London and Hong Kong

7. A company registered in the US that offers a film-streaming app across the globe

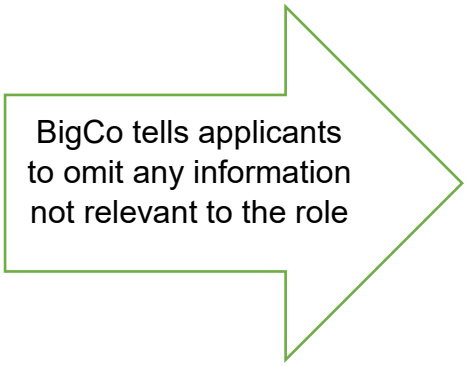
8. A global social media site passing data to a company owned by a US political lobbyist

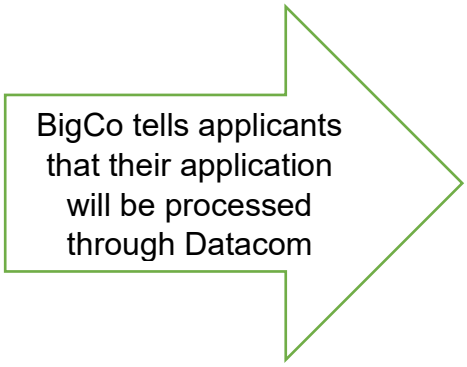
Exercise 3

BigCo is a publishing company, based in Wales. They publish magazines all over the world, and online. They are recruiting for the role of office manager for their Cardiff office. They place an advert on a career network site and invite applications via a portal called “Datacom”, a website where candidates are asked to upload their CV and details about their education and employment history, details of their suitability for the job, and names and contact details of references.

A. Match up the following FOUR statements with the corresponding principles under Article 5.

B. For the Article 5 principles not matched by one of the statements, think of an example to show how BigCo could comply with them. (For example, if you think the storage limitation principle does not feature in one of the 4 statements below, write a statement that could show how BigCo could comply with that principle).





Exercise 4

Match the following examples to a lawful basis. Note, there are more than one of the same!

1. A hospital trust asks staff to declare whether they have any COVID-19 symptoms

2. A movie-streaming app sends notifications to customers to tell them their subscription is due to end

3. A government authority collects data about asylum seekers to ensure they are able to access local services

4. A bank sends customers a bank statement

5. An online retailer sends emails to its customers about its latest products

6. A paramedic asks what medication a person who has collapsed has taken

7. A town council sends emails to local residents about events in the community

8. The payroll department of a police force collects staff data to make tax deductions from their

9. A local authority shares personal data to respond to a severe local flooding

Exercise 5

Which of the following items are examples of how organisations can comply with their obligations under Articles 24-39?

1. A policy for staff on data handling

2. A contract with a data processor

3. A Data Protection Officer

4. Use of secure a payment card standard for web purchases

5. A marketing director

6. An accountancy system to ensure invoices are paid on time

7. A risk report to the board of directors

8. A risk assessment on the use of CCTV

Exercise 6

BigCo has partnerships with a number of organisations. In each case, identify which of the following are processors, controllers, and joint controllers.

A A payroll company that provides payroll services to BigCo.

B A website hosting company that drops cookies on the devices of visitors to BigCo's websites.

C An events management company that pays BigCo for subscriber data and targets them with marketing about exhibitions they may be interested in.

D A local police force that monitors break-ins in the locality where BigCo's Cardiff office is.

E A travel agency that is running a competition with BigCo in their magazines for readers to enter and win a holiday.

F Pension scheme administrators that administer the pension scheme for BigCo's staff.

Exercise 7

A multinational car company based in the UK would like to send customer data to Germany for data analysis.

a) Which transfer mechanisms would be available to the car company?

b) Which of these would require a transfer risk assessment?

1. Binding Corporate Rules

2. International Data Transfer Agreement

3. International data transfer UK addendum to the EU's standard contractual clauses

4. Adequacy

5. Contractual clauses authorised by the ICO

5. Contractual clauses authorised by the ICO

6. Approved code of conduct

7. A legally binding and enforceable document

Exercise 8

Carla applies for the role of Office Manager but is rejected as her application did not meet the requirements of the “SelectBot”, a tool devised by Datacom that automatically weeds out any applications that do not appear to meet the basic criteria. She is informed that her application will be retained on BigCo’s records for six months, after which it will be archived for a further two years in case any future roles come up.

a) Which DSRs are available to Carla to exercise?

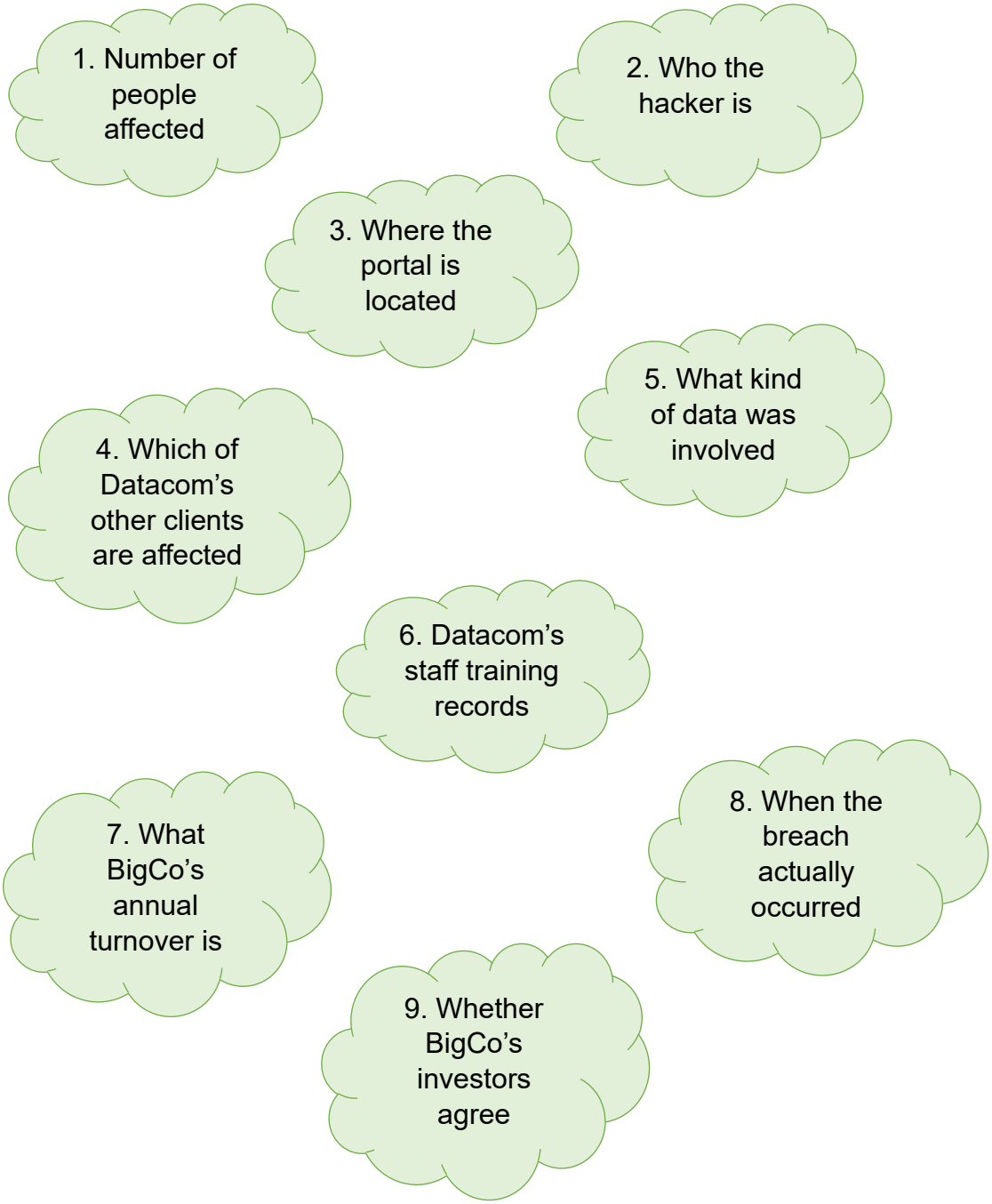
b) Which DSRs would already have been complied with by BigCo and how?

c) If it was identified that the "SelectBot" used AI what datasets would need to be checked to ensure Carla’s data rights were fulfilled correctly?

d) What mitigations would you consider to ensure a fair outcome for candidates like Carla?

Exercise 9

Unfortunately, Datacom suffers a massive data breach caused by a hacker exploiting a vulnerability in the portal site. What further information do you need to determine whether BigCo needs to report the breach to the ICO?



Exercise 10

Which of the following fall within PECR? For each that does fall within PECR, state whether opt-in or opt-out consent is required.

A. A cosmetics company wishes to sending marketing emails to followers of a beauty celebrity's Instagram page.

B. A vacuum cleaner retailer wishes to send marketing offers about its new vacuum cleaner to existing customers through the post.

C. A telemarketing company cold calls random phone numbers about the possibility that they may want to make a claim for being mis-sold an insurance product.

D. A streaming app sends notifications to subscribers' devices informing them their annual subscription is due to end and gives details of how to renew.

E. A political party uses local campaigners to put leaflets through the letterboxes of all residents in their area.

F. A car manufacturer places adverts on television at 8pm which is when it believes the majority of its potential customers will be viewing television.

G. A local council asks service users to sign up to its email newsletter to find out more about what's on in the community.

H. An accountancy practice wants to sell its list of customers to an insurance broker who specialises in business insurance.

I. A travel agency wants to send marketing email to customers regarding a new airport bus shuttle service it is running.

J. A drinks brand wants to send emails to previous entrants for a holiday competition about a new range of biscuits it is launching.

K. A registered animal charity wishes to send a fundraising email to an individual who previously donated to them and did not opt out.

Answers

<table>
<tr><th>Question</th><th colspan="2">Answer</th></tr>
<tr><td rowspan="2">Exercise 1</td><td>Binding
ECHR
Convention 108
EU GDPR
Charter of Fundamental Rights
PECR
Data Protection Act 2018
UK GDPR</td><td>Non-binding
UDHR
OECD Guidelines
Data Protection Directive
E-Privacy Directive</td></tr>
<tr><td colspan="2">World: UDHR, OECD Guidelines, Convention 108.

Europe: ECHR, Data Protection Directive, Charter of Fundamental Rights, E-Privacy Directive, EU GDPR.
UK: Data Protection Act 1998, PECR, Data Protection Act 2018, UK GDPR.</td></tr>
<tr><td>Exercise 2</td><td colspan="2">All of them fall within the GDPR.

Articles 3(1): 1, 2, 3, 4, 5, 6 (London office only)
Article 3(2)(a): 7
Article 3(2)(b): 8</td></tr>
<tr><td>Exercise 3</td><td colspan="2">A. Data minimisation, Lawful, fair, transparent processing, Storage limitation, Integrity and confidentiality.

B. Free text for discussion</td></tr>
</table>

Exercise 4	1. Legitimate interests. Vital interests might also be arguable. 2. Contractual obligation. 3. Public task or legal obligation (under immigration and equality legislation). Vital interests could also be argued. 4. Contractual obligation. Possibly also legal obligation under banking legislation. 5. Consent. Legitimate interests might also be arguable. 6. Vital interests. 7. Consent. Legal obligation (community cohesion) might also be arguable. NOT public task, as this is not something being done in the course of their official public duties. 8. Legal obligation (tax legislation). Contractual obligation also arguable. NOT public task. 9. Recognised Legitimate Interests.
Exercise 5	Yes – 1, 2, 3, 4 No – 5, Maybe 7 if it includes risks about data protection. Possibly 8 if it includes personal data images. Maybe 6 if the system holds bad debt details of customers (personal or sole trader) and it needs to go through a DPIA.
Exercise 6	Processors – A, B Controllers – C, D, F Joint controllers – E

Exercise 7	As Germany is a country based in the EEA which has adequacy, this option would be available. The company could also rely on Binding corporate rules, International data transfer addendum to the EU's standard contractual clauses, IDTA, Contractual clauses or a legally binding and enforceable document. If the company relies on adequacy then a transfer risk assessment does not need to take place. If they rely on any of the other transfer mechanisms then they would need to complete a transfer risk assessment first.
Exercise 8	A. Subject Access (Article 15), Rectification (Article 16), Erasure (Article 17), Objection (Article 21), Review of automated decision-making (Article 22). B. Right to Information / Transparency (Articles 13 & 14), by BigCo publishing a privacy notice. C. Right to obtain human intervention, express their point of view, and contest the automated decision (Articles 22A–22D). D. Auditing a percentage of all rejected applications. Thorough user testing before "go live". Allowing a candidate a review process. Making changes to the system based on audit findings, increase in number of complaints, or potential rights requests in this area.
Exercise 9	1, 5, 6, 8 All of the information is of course useful for context, but only 1, 5, 6 and 8 are required.
Exercise 10	A (opt-in), D (opt-out), G (opt-in), I (opt-out), J (opt-in), K Opt-out (relies on the charity soft opt-in)