BCS Practitioner Certificate in Data Protection v9.9

Exercise booklet

Contents

Document version history

Document version	Changes made
1.0 April 2026	Document created

Exercise 1

a) List all the relevant instruments, conventions, laws and declarations that have applied over time to protecting the right to privacy, in chronological order. For each one, specify which of these are binding, and whether they apply globally, in Europe, or just the UK.

b) Can you explain what is different about the GDPR compared to previous legislation in terms of how it applies in the EU?

Exercise 2

E-Bikes 4U is a major global retailer of electric and hybrid bikes. They have been told by an external GDPR consultant that they have to change some of their practices in order to ensure that they are compliant with the GDPR principles. Can you work out which of the GDPR principles the following activities relate to?

1. Delete the databases that hold absence data for former members of staff

2. Inform customers that E-Bikes 4U is collecting data about them in order to target them with the right products

3. Create a list of all processing activities with links to privacy notices sent to customers

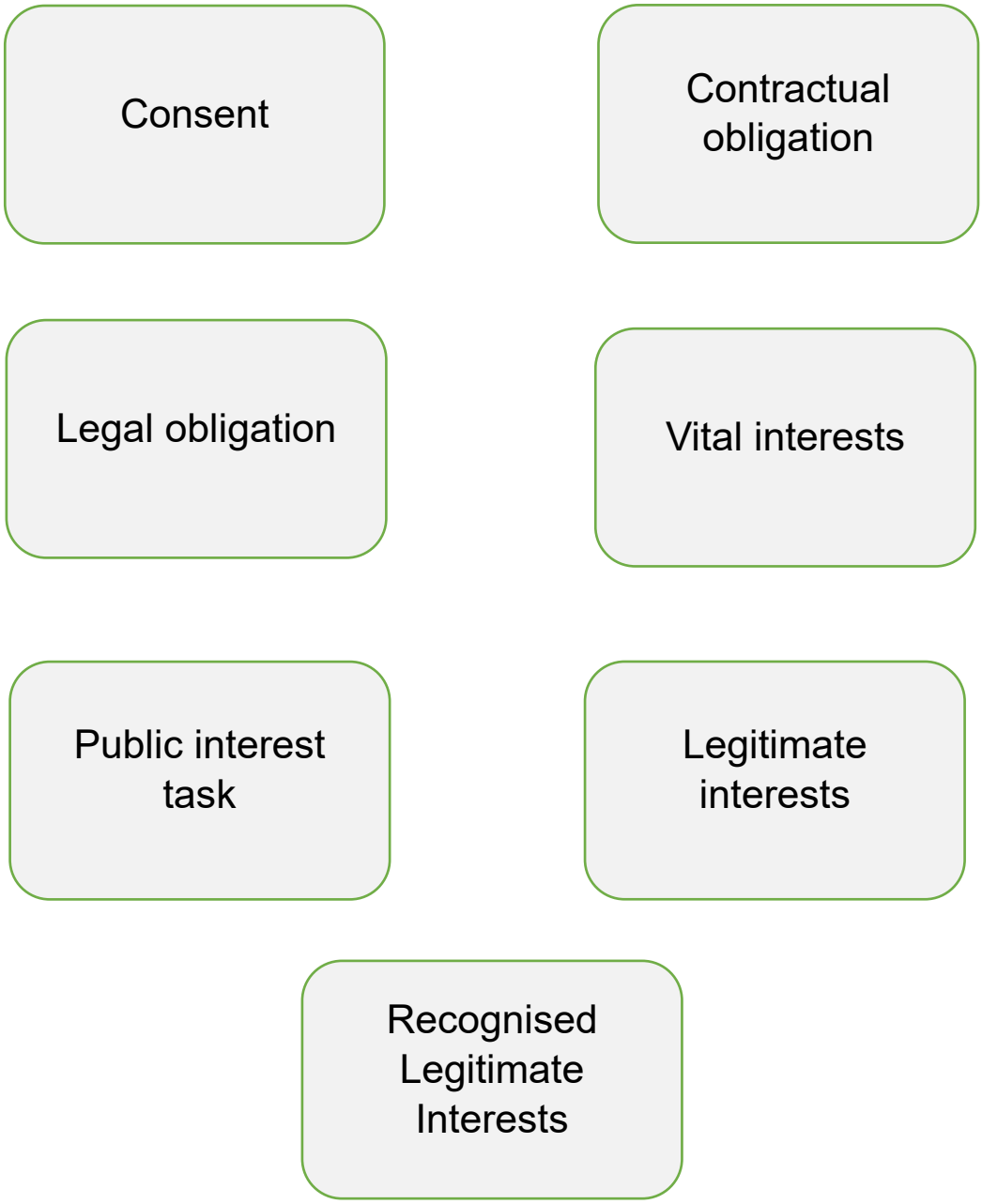
4. Deploy multi-factor authentication for staff accessing the company's network from home

5. Delete medical questionnaires from candidates who applied for roles but were never shortlisted

6. Update contact details for customers

Exercise 3

What kind of processing activities would E-Bikes 4U be carrying out? Think of one activity for each of the lawful bases that are available to them.



Exercise 4

Which of the following items are examples of how E-Bikes 4U 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 (DPO)	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 5

E-Bikes 4U 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.

b) A website hosting company that drops cookies on the devices of visitors to E-Bikes 4U websites.

c) An outdoor pursuits company that pays E-Bikes 4U for subscriber data and targets them with marketing about events they may be interested in.

d) A local police force that monitors break-ins in the locality where E-Bikes 4U's London office is.

e) A magazine publisher that is running a competition with E-Bikes 4U in their magazines for readers to enter and win an electric bike.

f) Pension scheme administrators that administer the pension scheme for E-Bikes 4U staff.

Exercise 6

In-Sure Health Limited is a company based in the UK that provides health insurance to UK residents. The company has outsourced its claims management functions to a third-party company based in the USA. This involve the third-party company employees being given access to In-Sure Health Limited's IT systems, which contain their customers' personal data (including health data).

a) Which of the following mechanisms could In-Sure Health Limited rely on? (Tick all that apply)

- ❑ Adequacy regulations.
- ❑ Binding Corporate Rules.
- ❑ Standard Contractual Clauses.
- ❑ Exemptions (Derogations).
- ❑ None required, as data is not being transferred.

b) Alongside the above mechanism, what other steps should In-Sure Health Limited take to ensure a compliant transfer?

Exercise 7

Carla applies for the role of Office Manager at E-bikes 4U's Paris office, 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 mee the basic criteria. She is informed that her application will be retained on E-Bikes 4U's records for 6 months, after which it will be archived for a further 2 years in case any future roles come up.

a) Which data subject requests (DSRs) are available to Carla to exercise?

b) Which DSRs would already have been complied with by E-Bikes 4U, and how?

Exercise 8

Carla applies to have her data erased, however her email was never actioned for an unknown reason. Carla complains to CNIL, the French Independent Supervisory Authority (ISA). For each of the following statements, state whether they are true or false.

a) Carla cannot complain straight to CNIL; she must first complain to E-Bikes 4U's DPO.

b) Before determining whether E-Bikes 4U have failed to comply with the GDPR, CNIL must first consult the European Data Protection Board (EDPB) to see if any other decisions have been taken against E-Bikes 4U.

c) CNIL cannot fine E-Bikes 4U for not responding to Carla because they have not produced a code of conduct for erasure requests.

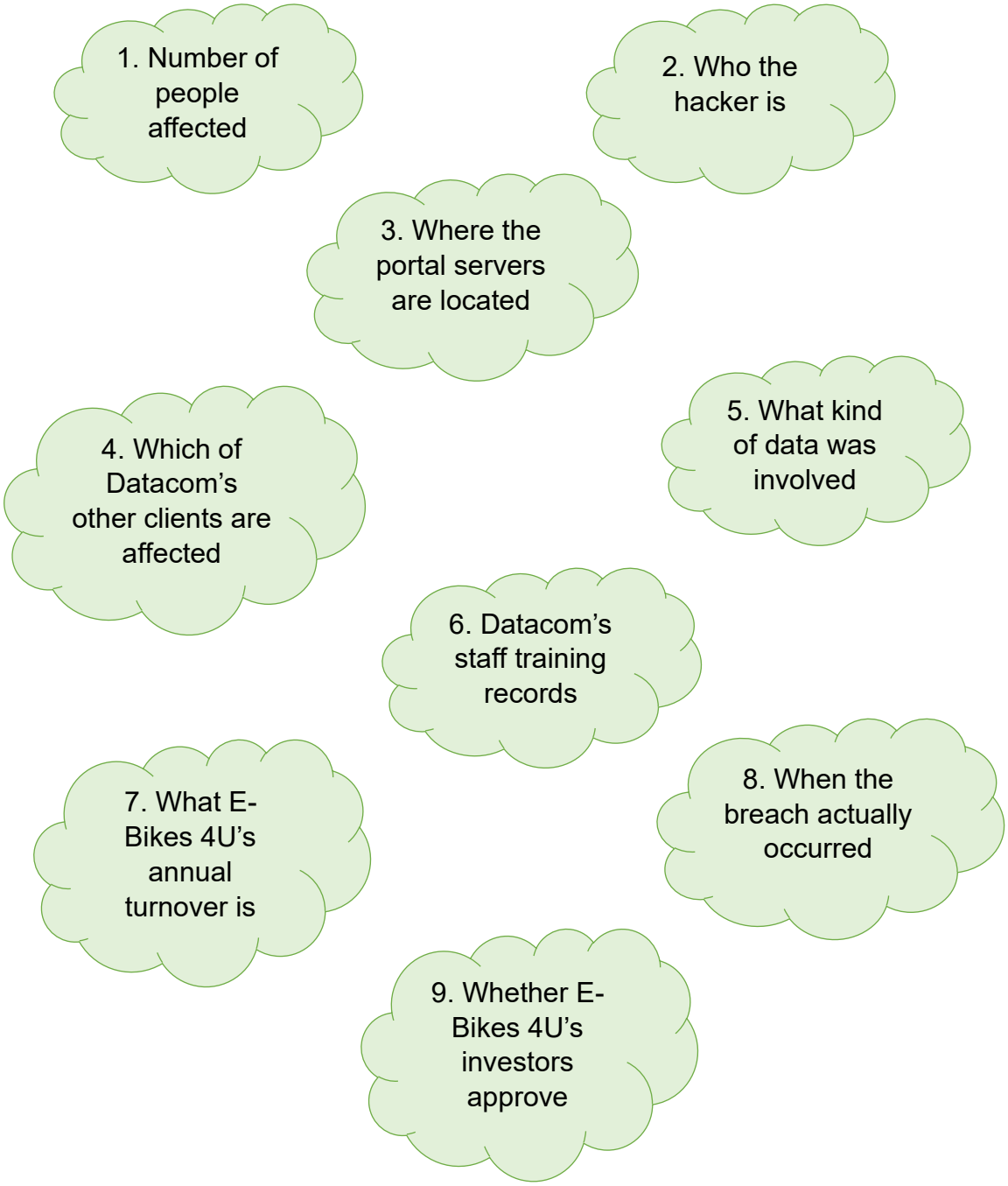
d) As E-Bikes 4U have offices in Madrid also, CNIL must apply to be a lead ISA before it can take any decision against E-Bikes 4U.

e) CNIL does not have any jurisdiction as E-Bikes 4U's email servers are located in New York.

f) CNIL can choose to raise Carla's complaint at the next meeting of the EDPB.

Exercise 9

Unfortunately, Datacom suffers a massive data breach, caused by a hacker exploiting a vulnerability in the recruitment portal site. It appears that every candidate who applied for any role across any of E-Bikes 4U's offices globally are affected. What further information do you need to determine whether E-Bikes 4U needs to report the breach to an ISA?



Exercise 10

Dylan is a 12-year-old boy, who lives in Manchester, UK. He decides to sign up for an online gaming service, which costs £8 per month. Dylan uses his own bank account, which was set up for him by his parents.

The service collects Dylan's personal data (including date of birth and bank details) when he signs up. The website asks for Dylan's consent to process this personal data.

For each of the following statements, indicate if they are true or false:

a) The service can process Dylan's personal data, because they have his consent.

b) The service does not need Dylan's parents' consent, because he has used his own bank details.

c) The service is not allowed to process Dylan's personal data as he is under 13.

d) The service must gain the consent of Dylan's parents as he is under 13.

e) The service must identify a special category condition, as Dylan's personal data is sensitive.

Exercise 11

Which of the following fall within the Privacy and Electronic Communications Regulations (PECR) (2003)? 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.

Exercise 12

An education authority is considering whether to use facial recognition technology to identify pupils at the cash register at lunch. This would be implemented to enable the deduction of money from an online account to reduce the need for children to bring cash for meals/snacks/drinks etc.

Identify the data protection requirements that arise from this proposition and suggest the actions/guidance you would offer as part of the data privacy team for the education authority.

Exercise 13

A shopping centre, in conjunction with a missing persons charity, is considering deploying new surveillance system that will involve the use of Artificial Intelligence (AI) to identify missing individuals in crowds and alert the police.

Which of the following measures would **best** address the data protection concerns in this scenario?

a) Share all gathered data proactively with the police, to ensure accuracy.

b) Conduct a Data Protection Impact Assessment (DPIA) in conjunction with the missing persons charity, before deploying.

c) Only share the gathered data with the missing persons charity.

d) Update the shopping centre's online privacy notice to reflect the new technology.

Answers

<table>
<tr><th>Question</th><th colspan="2">Answer</th></tr>
<tr><td rowspan="3">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 colspan="2">b) The EU GDPR is a regulation which means it is directly applicable on Member States, and Member States do not need to pass domestic legislation on the key areas, which avoids the risk of it being inconsistently applied.</td></tr>
<tr><td>Exercise 2</td><td colspan="2">1. Storage limitation principle (Article 5 (1)(e)).
2. Fairness, lawfulness, transparency (Article 5(1)(a)).
3. Accountability (Article 5(2)).
4. Integrity and confidentiality (Article 5(1)(f)).
5. Data minimisation (Article 5(1)(c)).
6. Accuracy (Article 5(1)(d)).</td></tr>
</table>

Exercise 3	Free text for discussion. Examples include: Consent: marketing activities. Contractual obligation: payment details for customers. Legal obligation: tax deductions from staff salaries, to comply with tax legislation. Vital interests: next of kin contact details for staff in case of emergencies. Public interest task: not available. Legitimate interests: soft opt-in for marketing to existing customers, use of business systems for staff to use email and video conferencing facilities.
Exercise 4	Yes – 1, 2, 3, 4. No – 5, 6. Maybe – 7 if it includes risks about data protection, 8 if it includes personal data images.
Exercise 5	Processors – A, B. Controllers – C, D, F. Joint controllers – E.
Exercise 6	a) Standard Contractual Clauses. No other option is suitable for this arrangement: • Adequacy: US is not currently adequate. • BCRs: Only applicable to a corporate group. • Derogations: Not suitable for systematic transfer of data. • None required: Access from a third country is considered a 'transfer', therefore a mechanism is required. b) Looking for the learner to identify any (ideally, all) of the following: • Article 28 Data Processing Agreement (as the third-party will be a data processor). • Conduct a Data Protection Impact Assessment (due to potential high risk). • Conduct a Transfer Risk Assessment (as the US is not currently an adequate country). Other answers by the learner should be considered, and learners should not be penalised for identifying other valid options (e.g. cyber

	security test, non-disclosure agreement, etc.).
Exercise 7	a) Right to obtain human intervention, express their point of view, and contest the automated decision (Articles 22A–22D). b) Right to information / transparency (Articles 13 & 14), by E-Bikes 4U publishing a privacy notice.
Exercise 8	All false, except for F.
Exercise 9	1, 5, 8.
Exercise 10	For each of the following statements, indicate if they are true or false: • The service can process Dylan's personal data, because they have his consent. FALSE. Dylan is under the age of consent in the UK & EU GDPR (13, 16 respectively). • The service does not need Dylan's parents' consent, because he has used his own bank details. FALSE. The fact he has used his own bank details is irrelevant. • The service is not allowed to process Dylan's personal data as he is under 13. FALSE. There is no general restriction on the processing of children's data. • The service must gain the consent of Dylan's parents as he is under 13. TRUE. Article 8 of the UK GDPR states that parental consent must be gained for information society services. • The service must identify a special category condition, as Dylan's personal data is sensitive. FALSE. Dylan's personal data is not special category data because he is a child.
Exercise 11	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).

Exercise 12	Facial recognition technology would involve processing pupil special category data. A DPIA should be carried out before commencing processing. The Education Authority must be able to evidence that facial recognition technology is a necessary and proportionate way to manage payments for a school lunch service and whether less intrusive alternatives are available. If a third-party provider (processor) is to be engaged, there should be adequate due diligence and an agreed contract with appropriate data protection clauses in place before they are given data. Because this is aimed at children, there needs to be consideration of whether they will understand the risks. Any privacy policy needs to be briefed in simple language. Lawful basis of processing needs to be agreed; consent would need a decision on whether it was from the child or the parent. As biometric needs an Article 9 condition for processing, explicit consent is the only condition available. Education authorities in England and Wales must also apply the Protection of Freedoms Act 2012 which sets out rules about parental and child consent for the use of biometrics in schools. These must be in place alongside data protection requirements. Processes must be in place for deletion of personal data and also for ensuring the data is maintained accurately, securely and that only relevant information is kept. There should also be processes in place to ensure that the children and parents know how to exercise their data rights.
Exercise 13	a) This action may actively aggravate the data protection concerns. b) This is the most appropriate course of action, as it will encourage the shopping centre and the charity to consider the necessity, proportionality and possible risks of this new processing activity. c) This will help, but does not address the other concerns around accuracy, purpose, security, proportionality, privacy etc. d) This is a minor step towards ensuring transparency but does not represent a meaningful move towards ensuring that visitors are aware of this processing.