BCS PRACTITIONER CERTIFICATE IN DATA PROTECTION

COURSEWARE

EXERCISE BOOKLET

The Chartered Institute for IT

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, and 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 it 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

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

Circle 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

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

2. A contract with a

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

3. A Data Protection Officer

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

A Match the key characteristics to each of the transfer mechanisms:

Binding Corporate Rules	Only applies to intra-company transfers
Standard Contractual Clauses	Applies to an entire country's processing activities
Adequacy	Easy to adopt

B E-Bikes 4U's offices are also located in New York, Tokyo, Paris and Brisbane. Which mechanisms could apply to each of these? List all that could apply.

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 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 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 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.**

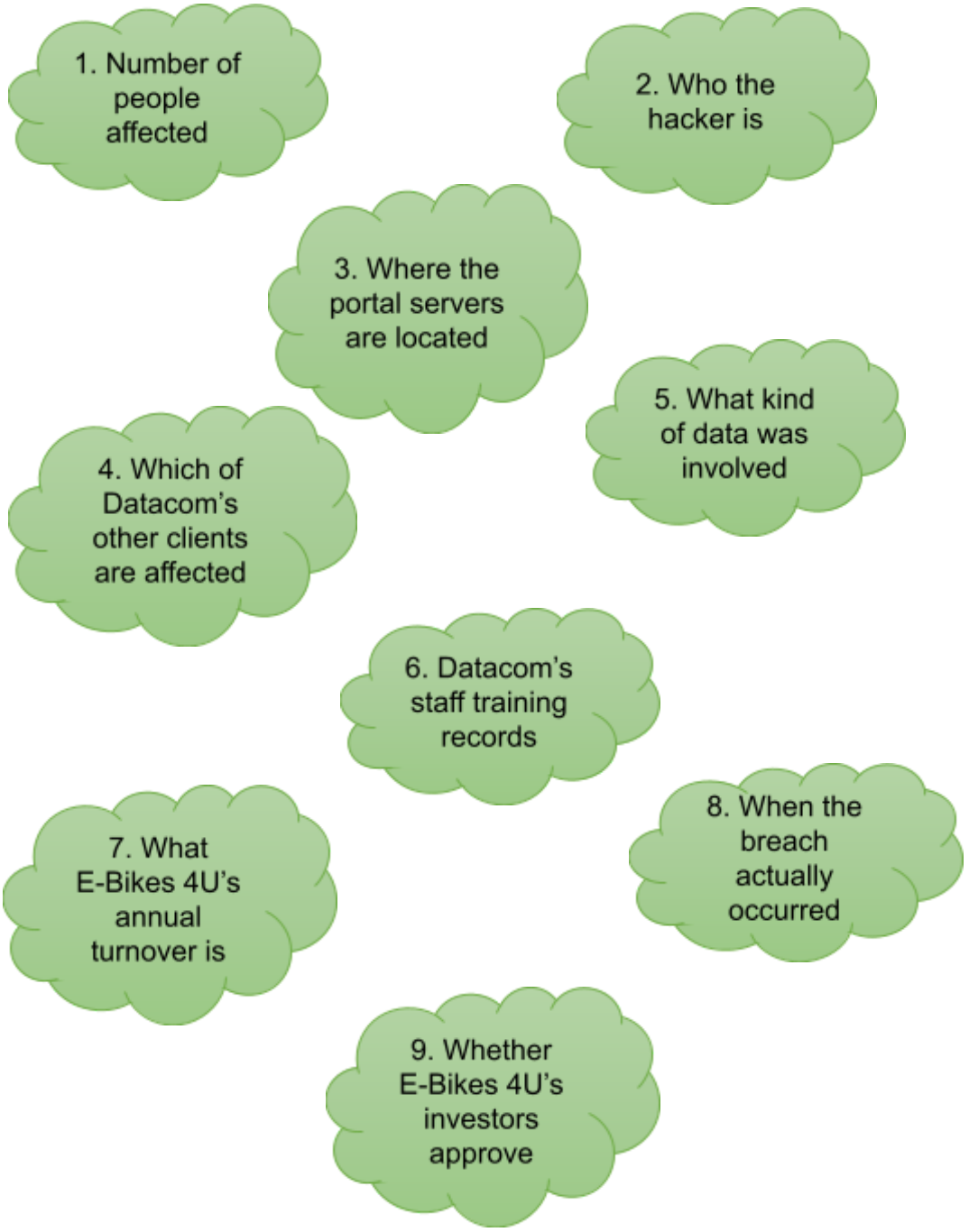
D. **As E-Bikes 4U have offices in Madrid also, CNIL must apply to be a lead ISA before it can take any decision against E-Bikes 4U.**

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

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**

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 EY 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 (Art 5 (1)(e))
2. fairness, lawfulness, transparency (Art 5(1)(a))
3. accountability (Art 5(2))
4. integrity and confidentiality (Art 5(1)(f))
5. data minimisation (Art 5(1)(c))
6. accuracy (Art 5(1)(d))</td></tr>
<tr><td>Exercise 3</td><td colspan="2">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</td></tr>
<tr><td>Exercise 4</td><td colspan="2">Yes – 1, 2, 3, 4</td></tr>
</table>

	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. 1 1; 2 3; 3 2 B. New York: Standard Contractual Clauses, Binding Corporate Rules Tokyo: Adequacy, Standard Contractual Clauses, Binding Corporate Rules Paris: Standard Contractual Clauses, Binding Corporate Rules Brisbane: Standard Contractual Clauses, Binding Corporate Rules
Exercise 7	A. Subject Access (Art 15), Rectification (Art 16), Erasure (Art 17), Restriction (Art 18), Objection (Art 21), Review of automated decision-making (Art 22) B. Right to Information / Transparency (Arts 13 & 14), by E-Bikes 4U publishing a privacy notice
Exercise 8	All false, except for F.
Exercise 9	1, 5, 8
Exercise 10	A (opt-in), D (opt-out), G (opt-in), I (opt-out), J (opt-in)