CERTLABZ CERTIFICATION BOARD

Certified Data Privacy Professional (CDPP)

Ten Sample Questions

These ten questions are written at the difficulty of the live exam. Six carry a figure, a data table, a configuration or a code listing; four are plain scenario questions, as on the live paper. Every one is a scenario a working data privacy professional would meet, and none of them appears in the live question bank.

The live exam is multistage adaptive: how you score on one stage selects the difficulty of the next, so no two candidates sit the same paper. It is a performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions, which means you build, sequence or complete something rather than only choosing from a list. Answers and full explanations follow each question here; the live exam does not disclose item-level answers.

Question 1 — Domain 1: Data Privacy Foundations — DATA

Sarah Miller maps each privacy term to its meaning, with one meaning missing.

Term	Meaning
Personal data	Info about a person
Processing	(to choose)
Data subject	The person involved
Anonymisation	Cannot re-identify

Table 1.1 Core privacy terms.

What does processing mean?

A. Only deleting files
B. Any use of the data
C. Selling to brokers
D. Encrypting at rest

Correct answer: B

Processing covers any operation on personal data, from collection and storage to use and erasure, so it means any use of the data. The other options each name a single narrow action rather than the broad definition.

Question 2 Domain 2: Regulations and Frameworks DATA

James Carter maps each role to what it does, with one duty missing.

Role	Duty
Controller	Decides why and how
Processor	(to choose)
Data subject	The person involved
Supervisory body	Enforces the rules

Table 2.1 Privacy roles and duties.

What does the processor do?

- A Sets all the purposes
- B Acts for the controller
- C Files the complaints
- D Writes the whole law

Correct answer: B
A processor handles personal data on behalf of and under the instructions of the controller, so it acts for the controller. The controller sets the purposes and means, while the other options describe subjects or regulators.

Question 3 Domain 3: Data Subject Rights DATA

Emma Wilson maps each request to the right it uses, with one right missing.

Request	Right
Get a copy	Access
Fix a mistake	Rectification
Delete my data	(to choose)
Move to rival	Portability

Table 3.1 Requests and rights.

Which right covers deletion?

- A Right to object
- B Right to erasure
- C Right to restrict
- D Right to be told

Correct answer: B
The right to erasure, also called the right to be forgotten, lets a person ask that their data be deleted when grounds apply. Objection stops certain uses, restriction pauses processing, and the right to be told covers notice.

Question 4

Domain 5: Consent, Data Mapping and DPIAs

CONFIG

David Brown reviews a records-of-processing entry for a marketing list.

```
activity:   email marketing
purpose:    send promotions
categories: name, email
lawful_basis: consent
retention:  24 months
```

Listing 4.1 A processing record.

What justifies this processing?

A. Legitimate interest
B. A signed contract
C. The lawful basis
D. A legal duty

Correct answer: C
Every processing activity needs a documented lawful basis, and this record names consent as the basis for the marketing use. The other options list bases that could apply elsewhere but are not the one recorded here.

Question 5

Domain 5: Consent, Data Mapping and DPIAs

CONFIG

Olivia Davis reviews the consent banner settings before launch.

```
analytics:   default = off
marketing:   default = off
necessary:   always on
granular:    true
withdraw:    one click
```

Listing 5.1 Consent settings.

Why are non-essential defaults off?

A. To speed the page up
B. Consent must be opt in
C. To save on storage
D. The law bans banners

Correct answer: B
Valid consent must be a clear affirmative act, so non-essential categories default to off until the person opts in. Necessary cookies stay on because they are not consent based, and the other options miss the consent rule.

Question 6

Domain 6: Breach, Governance and Accountability

DATA

Ava Thompson maps each breach step to its owner, with one owner missing.

Step	Owner
Spot the breach	Any staff member
Assess the risk	Privacy office
Notify regulator	(to choose)
Tell affected users	Comms team

Table 6.1 Breach steps and owners.

Who notifies the regulator?

A. The vendor helpdesk
B. Any single user
C. The data controller
D. The web host only

Correct answer: C
The controller holds accountability for the data and must report a qualifying breach to the supervisory body within the deadline. Staff report internally and comms informs users, but the regulator notice sits with the controller.

Question 7

Domain 1: Data Privacy Foundations

A team collects birth dates for a newsletter signup when only an email is needed to send it, keeping the extra field just in case. Which principle does this break?

A. Data minimisation
B. Storage forever
C. Open by default
D. More is safer

Correct answer: A
Data minimisation means collecting only what the stated purpose needs, so gathering birth dates for a plain newsletter breaks it. Keeping fields just in case raises risk without a purpose, which the principle exists to prevent.

Question 8 Domain 2: Regulations and Frameworks

A company assumes one privacy notice written for one region automatically satisfies every law worldwide, so it never checks local rules. What is the sound approach?

A One notice fits all

B Ignore other regions

C Map to each regime

D Wait for a fine

Correct answer: C
Privacy laws such as GDPR and CCPA differ in scope, rights and notices, so a program should map its obligations to each regime it falls under. Assuming one notice covers the world leaves gaps that surface only when a regulator or user acts.

Question 9 Domain 4: Privacy by Design

A new app is built first and privacy is bolted on just before launch, so consent and data limits are hard to retrofit. What does privacy by design require?

A Add it at the end

B Build it in early

C Skip it for speed

D Leave it to legal

Correct answer: B
Privacy by design means building safeguards into a system from the start rather than bolting them on late. Early design lets consent, minimisation and defaults shape the architecture, which retrofitting near launch cannot do cleanly.

Question 10 Domain 3: Data Subject Rights

A person asks to see all the data a firm holds on them, but the firm ignores the request because it is busy and has no set process. What right is being denied?

A Right of access

B Right to profit

C Right to reply

D Right to hide

Correct answer: A
The right of access lets a person obtain a copy of the personal data held about them within a set time. Ignoring the request denies that right, and firms need a documented process to respond rather than treating it as optional.

CDPP-001. https://certlabz.com/certifications/certified-data-privacy-professional.html