

CIPM^{Q&As}

Certified Information Privacy Manager





Pass IAPP CIPM Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/cipm.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

Under the General Data Protection Regulation (GDPR), what obligation does a data controller or processor have after appointing a Data Protection Officer (DPO)?

- A. To submit for approval to the DPO a code of conduct to govern organizational practices and demonstrate compliance with data protection principles.
- B. To provide resources necessary to carry out the defined tasks of the DPO and to maintain their expert knowledge.
- C. To ensure that the DPO acts as the sole point of contact for individuals' questions about their personal data.
- D. To ensure that the DPO receives sufficient instructions regarding the exercise of their defined tasks.

Correct Answer: B

QUESTION 2

Which of the following best describes proper compliance for an international organization using Binding Corporate Rules (BCRs) as a controller or processor?

- A. Employees must sign an ad hoc contractual agreement each time personal data is exported.
- B. All employees are subject to the rules in their entirety, regardless of where the work is taking place.
- C. All employees must follow the privacy regulations of the jurisdictions where the current scope of their work is established.
- D. Employees who control personal data must complete a rigorous certification procedure, as they are exempt from legal enforcement.

Correct Answer: A

Reference: <https://www.lexology.com/library/detail.aspx?g=80239951-01b8-409f-9019-953f5233852e>

QUESTION 3

SCENARIO

Please use the following to answer the next question:

Hi Zoe,

Thank you so much for your email. I am so glad you have jumped right into your new position as our in-house privacy professional. BastTech greatly needs your expertise. I hope you are comfortably settling into your new home in the United

States after your move from the United Kingdom! Georgia is a wonderful state.

I particularly appreciate your enthusiasm in using your recent informal assessment to begin rectifying gaps in our privacy program and making sure we are in compliance with all laws. However, I also want to make sure that we are prioritizing

our initiatives by spending time on the measures that are most important to our customers, our company, and the tech industry as a whole.

Specifically, I know that you are advocating for an update of our Business Continuity Disaster Response (BCDR) plan with an eye toward privacy concerns. I think this effort is something that we may be able to postpone. I'm sure that after ten

years the document can be updated in spots; however, we have first-rate, experienced executive leaders that would have things well in hand in the unlikely event of a disaster.

Further, you mentioned that you would like to assess our longtime subcontractor's disaster plan through a second-party audit. Papyrus, our longtime subcontractor, does keep a great deal of personal data about our customers. However, I am

not sure I understand your request and would like to discuss this further during our meeting Wednesday.

You also say that your audit uncovered some inadequacies in staff compliance with our security procedures and local laws. I just wanted to emphasize that the audit findings only need to be communicated to the executive leadership. I would

rather not cause unnecessary alarm across departments.

I know you are also looking closely at the recent loss of a file belonging to a staff member in Human Resources (HR). It was an unfortunate incident, but rest assured, we handled the situation according to Georgia state law. The only difficult part was easing the concerns of our many remote employees all across the country whose data was on the computer. But I believe everything is settled. At least this stands as proof that in the event of another breach of any type, Information

Security (IS) will take the lead while other departments move on with business as usual without having to get involved. Thankfully, we have taken the measure of supplementing our General Commercial Liability Insurance with cyber insurance.

Anyway, we will talk more on Wednesday. I just wanted to communicate some of my current thinking.

Thanks,

Whitney

Interim Assistant Business Manager, BastTech.

To better respond to privacy incidents, Whitney should consider making better use of what?

- A. An appropriate industry framework.
- B. Training offered outside the company.
- C. Protocols for amending personal data.
- D. Roles of stakeholders across departments.

Correct Answer: D

QUESTION 4

SCENARIO

Please use the following to answer the next QUESTION:

Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather's law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office's strategies for growth.

Immediately upon arrival, Richard was amazed at the amount of work that needed to be done in order to modernize the office, mostly in regard to the handling of clients' personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place. Richard is also concerned with the overuse of the communal copier/ printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year's end.

Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary. Mr. McAdams granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.

Which of the following policy statements needs additional instructions in order to further protect the personal data of their clients?

- A. All faxes sent from the office must be documented and the phone number used must be double checked to ensure a safe arrival.
- B. All unused copies, prints, and faxes must be discarded in a designated recycling bin located near the work station and emptied daily.
- C. Before any copiers, printers, or fax machines are replaced or resold, the hard drives of these devices must be deleted before leaving the office.
- D. When sending a print job containing personal data, the user must not leave the information visible on the computer screen following the print command and must retrieve the printed document immediately.

Correct Answer: D

QUESTION 5

"Respond" in the privacy operational lifecycle includes which of the following?

- A. Information security practices and functional area integration.

- B. Privacy awareness training and compliance monitoring.
- C. Communication to stakeholders and alignment to laws.
- D. Information requests and privacy rights requests.

Correct Answer: D

[CIPM PDF Dumps](#)

[CIPM VCE Dumps](#)

[CIPM Braindumps](#)