Free Questions for CIPM by vceexamstest

Shared by Morris on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

While trying to e-mail her manager, an employee has e-mailed a list of all the company's customers, including their bank details, to an employee with the same name at a different company. Which of the following would be the first stage in the incident response plan under the General Data Protection Regulation (GDPR)?

Options:

A- Notification to data subjects.

B- Containment of impact of breach.

C- Remediation offers to data subjects.

D- Notification to the Information Commissioner's Office (ICO).

Answer:

B

Explanation:

The first stage in the incident response plan under the General Data Protection Regulation (GDPR) for this scenario would be to contain the impact of the breach. This means taking immediate action to stop the unauthorized access or disclosure of personal data, and to prevent it from happening again in the future. This could involve revoking access to the data, notifying the employee who mistakenly sent the data, and implementing security measures to prevent similar breaches from occurring in the future.

https://gdpr-info.eu/art-33-gdpr/

https://gdpr-info.eu/art-34-gdpr/

Question 2

Question Type: **MultipleChoice**

A systems audit uncovered a shared drive folder containing sensitive employee data with no access controls and therefore was available for all employees to view. What is the first step to mitigate further risks?

Options:

A- Notify all employees whose information was contained in the file.

B- Check access logs to see who accessed the folder.

C- Notify legal counsel of a privacy incident.

D- Restrict access to the folder.

Answer:

D

Explanation:

The first step to mitigate further risks when a systems audit uncovers a shared drive folder containing sensitive employee data with no access controls is to restrict access to the folder. This can be done by implementing appropriate access controls, such as user authentication, role-based access, and permissions, to ensure that only authorized individuals can view and access the sensitive data.

https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492158151.pdf

https://www.itgovernance.co.uk/blog/5-reasons-why-employees-dont-report-data-breaches/

https://www.ncsc.gov.uk/guidance/report-cyber-incident

Question 3

Question Type: MultipleChoice

You would like to better understand how your organization can demonstrate compliance with international privacy standards and identify gaps for remediation. What steps could you take to achieve this objective?

Options:

A- Carry out a second-party audit.

B- Consult your local privacy regulator.

C- Conduct an annual self assessment.

D- Engage a third-party to conduct an audit.

Answer:

D

Explanation:

Engaging a third-party to conduct an audit is the best way to ensure that your organization is compliant with international privacy standards and identify any gaps that need to be remediated. An audit should include a review of your organization's data processing activities, as well as its policies, procedures, and internal controls. Additionally, it should include an analysis of the applicable privacy laws and regulations. This audit will provide you with an objective third-party assessment of your organization's compliance with international privacy standards and identify any areas of non-compliance that need to be addressed

Question 4

Question Type: MultipleChoice

Which of the following is NOT recommended for effective Identity Access Management?

Options:

A- Demographics.

B- Unique user IDs.

C- User responsibility.

D- Credentials (e.g.. password).

Answer:

A

Explanation:

Identity and Access Management (IAM) is a process that helps organizations secure their systems and data by controlling who has access to them and what they can do with that access. Effective IAM includes a number of best practices, such as:

Unique user IDs: Each user should have a unique ID that is used to identify them across all systems and applications.

Credentials: Users should be required to provide authentication credentials, such as a password or biometric data, in order to access systems and data.

User responsibility: Users should be made aware of their responsibilities when it comes to security, such as the need to keep their passwords secret and the importance of reporting suspicious activity.

Demographics refers to the statistical characteristics of a population, such as age, gender, income, etc. While demographic data may be collected and used for various purposes, it is not a recommended practice for effective IAM. Demographic data is not a reliable method of identification or authentication, and it is not used to provide access to systems and data.

https://aws.amazon.com/iam/

https://en.wikipedia.org/wiki/Identity_and_access_management

https://en.wikipedia.org/wiki/Demographics

Question 5

Question Type: MultipleChoice

If done correctly, how can a Data Protection Impact Assessment (DPIA) create a win/win scenario for organizations and individuals?

Options:

A- By quickly identifying potentially problematic data attributes and reducing the risk exposure.

B- By allowing Data Controllers to solicit feedback from individuals about how they feel about the potential data processing.

C- By enabling Data Controllers to be proactive in their analysis of processing activities and ensuring compliance with the law.

D- By better informing about the risks associated with the processing activity and improving the organization's transparency with individuals.

Answer:

D

Explanation:

A Data Protection Impact Assessment (DPIA) is a process that organizations use to evaluate the potential risks associated with a specific data processing activity, and to identify and implement measures to mitigate those risks. By conducting a DPIA, organizations can proactively identify and address potential privacy concerns before they become a problem, and ensure compliance with data protection laws and regulations.

When organizations are transparent about their data processing activities and the risks associated with them, individuals are better informed about how their personal data is being used and can make more informed decisions about whether or not to provide their personal data. This creates a win/win scenario for organizations and individuals, as organizations are able to continue processing personal data in a compliant and transparent manner, while individuals are able to trust that their personal data is being used responsibly.

Additionally, by engaging with individuals in the DPIA process and soliciting their feedback, organizations can better understand the potential impact of their data processing activities on individuals and take steps to mitigate any negative impacts.

-https://ec.europa.eu/info/publications/data-protection-impact-assessment-dpia-guidelines_en -https://gdpr-info.eu/art-35-gdpr/

Question 6

Question Type: MultipleChoice

When devising effective employee policies to address a particular issue, which of the following should be included in the first draft?

Options:

A- Rationale for the policy.

B- Points of contact for the employee.

C- Roles and responsibilities of the different groups of individuals.

D- Explanation of how the policy is applied within the organization.

Answer:

B

Question 7

Question Type: MultipleChoice

Which of the following actions is NOT required during a data privacy diligence process for Merger & Acquisition (M&A) deals?

Options:

A- Revise inventory of applications that house personal data and data mapping.

B- Update business processes to handle Data Subject Requests (DSRs).

C- Compare the original use of personal data to post-merger use.

D- Perform a privacy readiness assessment before the deal.

Answer:

D

Question 8

Question Type: MultipleChoice

When building a data privacy program, what is a good starting point to understand the scope of privacy program needs?

Options:

A- Perform Data Protection Impact Assessments (DPIAs).

B- Perform Risk Assessments

C- Complete a Data Inventory.

D- Review Audits.

Answer:

C

Question 9

Question Type: MultipleChoice

When supporting the business and data privacy program expanding into a new jurisdiction, it is important to do all of the following EXCEPT?

Options:

A- Identify the stakeholders.

B- Appoint a new Privacy Officer (PO) for that jurisdiction.

C- Perform an assessment of the laws applicable in that new jurisdiction.

D- Consider culture and whether the privacy framework will need to account for changes in culture.

Answer:

D

Question 10

Question Type: MultipleChoice

Which of the following is NOT an important factor to consider when developing a data retention policy?

Options:

A- Technology resource.

B- Business requirement.

C- Organizational culture.

D- Compliance requirement

Answer:

A

Question 11

Question Type: MultipleChoice

Which of the following helps build trust with customers and stakeholders?

Options:

A- Only publish what is legally necessary to reduce your liability.

B- Enable customers to view and change their own personal information within a dedicated portal.

C- Publish your privacy policy using broad language to ensure all of your organization's activities are captured.

D- Provide a dedicated privacy space with the privacy policy, explanatory documents and operation frameworks.

Answer:

C