Free Questions for CIPM by go4braindumps

Shared by Anderson on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SCENARIO

Please use the following to answer the next question

You were recently hired by InStyte Date Corp as a privacy manager to help InStyle Data Corp become compliant with a new data protection law

The law mandates that businesses have reasonable and appropriate security measures in place to protect personal dat

a. Violations of that mandate are heavily fined and the legislators have stated that they will aggressively pursue companies that don t comply with the new law

You are paved with a security manager and tasked with reviewing InStyle Data Corp s current state and advising the business how it can meet the "reasonable and appropriate security" requirement InStyle Data Corp has grown rapidly and has not kept a data inventory or completed a data mapping InStyte Data Corp has also developed security-related policies ad hoc and many have never been implemented The various teams involved in the creation and testing of InStyle Data Corp s products experience significant turnover and do not have well defined roles There's little documentation addressing what personal data is processed by which product and for what purpose

Work needs to begin on this project immediately so that InStyle Data Corp can become compliant by the time the law goes into effect. You and you partner discover that InStyle Data Corp regularly sends files containing sensitive personal data back to its customers through email sometimes using InStyle Data Corp employees personal email accounts. You also team that InStyle Data Corp s privacy

and information security teams are not informed of new personal data flows, new products developed by InStyte Data Corp that process personal data, or updates to existing InStyle Data Corp products that may change what or how the personal data is processed until after the product or update has gone have.

Through a review of InStyle Date Corp's test and development environment logs, you discover InStyle Data Corp sometimes gives login credentials to any InStyle Data Corp employee or contractor who requests them. The test environment only contains dummy data but the development environment contains personal data including Social Security Numbers, hearth ^formation and financial information All credentialed InStyle Data Corp employees and contractors have the ability to after and delete personal data in both environments regardless of their role or what project they are working on.

You and your partner provide a gap assessment citing the issues you spotted, along with recommended remedial actions and a method to measure implementation InStyle Data Corp implements all of the recommended security controls You review the processes roles, controls and measures taken to appropriately protect the personal data at every stop However, you realize there is no plan for monitoring and nothing in place addressing sanctions for violations of the updated policies and procedures InStyle Data Corp pushes back, stating they do not have the resources for such monitoring.

Having completed the gap assessment, you and your partner need to first undertake a thorough review of?

Options:

A- Data life cyde

B- Security policies.

C- System development life cycle.

D- Privacy Impact (PIA).

Answer:

C

Explanation:

Having completed the gap assessment, you and your partner need to first undertake a thorough review of the system development life cycle (SDLC). This is because the SDLC is the process of creating, testing, deploying, and maintaining software products, which involves the processing of personal data by InStyle Data Corp. A review of the SDLC will help you identify and address the privacy and security risks and requirements at each stage of the development process, such as design, coding, testing, and deployment. The other options are not the first things that you need to review, as they are either part of the gap assessment (security policies) or the outcome of the review (data life cycle and privacy impact assessment).

Question 2

Question Type: **MultipleChoice**

SCENARIO

Please use the following to answer the next question

You were recently hired by InStyte Date Corp as a privacy manager to help InStyle Data Corp become compliant with a new data protection law

The law mandates that businesses have reasonable and appropriate security measures in place to protect personal data. Violations of that mandate are heavily fined and the legislators have stated that they will aggressively pursue companies that don t comply with the new law

You are paved with a security manager and tasked with reviewing InStyle Data Corp s current state and advising the business how it can meet the "reasonable and appropriate security" requirement InStyle Data Corp has grown rapidly and has not kept a data inventory or completed a data mapping InStyte Data Corp has also developed security-related policies ad hoc and many have never been implemented The various teams involved in the creation and testing of InStyle Data Corp s products experience significant turnover and do not have well defined roles There's little documentation addressing what personal data is processed by which product and for what purpose

Work needs to begin on this project immediately so that InStyle Data Corp can become compliant by the time the law goes into effect. You and you partner discover that InStyle Data Corp regularly sends files containing sensitive personal data back to its customers through email sometimes using InStyle Data Corp employees personal email accounts. You also team that InStyle Data Corp s privacy and information security teams are not informed of new personal data flows, new products developed by InStyte Data Corp that process personal data, or updates to existing InStyle Data Corp products that may change what or how the personal data is processed until after the product or update has gone have.

Through a review of InStyle Date Corp's test and development environment logs, you discover InStyle Data Corp sometimes gives login credentials to any InStyle Data Corp employee or contractor who requests them. The test environment only contains dummy data but the development environment contains personal data including Social Security Numbers, hearth ^formation and financial information All credentialed InStyle Data Corp employees and contractors have the ability to after and delete personal data in both environments regardless of their role or what project they are working on.

You and your partner provide a gap assessment citing the issues you spotted, along with recommended remedial actions and a method to measure implementation InStyle Data Corp implements all of the recommended security controls You review the processes roles, controls and measures taken to appropriately protect the personal data at every stop However, you realize there is no plan for monitoring and nothing in place addressing sanctions for violations of the updated policies and procedures InStyle Data Corp pushes back, stating they do not have the resources for such monitoring.

What aspect of the data management life cycle will still be unaddressed it you cannot find the resources to become compliant?

Options:

A- Auditability.

B- Enforcement

C- Irretrievability

D- Access management

Answer:

B

Explanation:

The aspect of the data management life cycle that will still be unaddressed if you cannot find the resources to become compliant is enforcement. Enforcement means ensuring that the data policies and procedures are followed by all data users and stakeholders, and

that any violations or deviations are detected, reported, and corrected. Enforcement also involves imposing sanctions or penalties for non-compliance, such as revoking access rights, issuing warnings, or terminating contracts. Without enforcement, the data security measures that you implemented may not be effective or sustainable, as there would be no accountability or deterrence for data misuse or abuse1, 2.

To address the enforcement aspect of the data management life cycle, you should try to convince InStyle Data Corp of the importance and benefits of monitoring and sanctioning data activities. You should explain that monitoring can help identify and prevent data breaches, errors, or inefficiencies, as well as demonstrate compliance with the new data protection law. You should also explain that sanctioning can help enforce data discipline and responsibility, as well as deter potential violators or malicious actors. You should also propose some possible ways to allocate or optimize the resources for monitoring and sanctioning, such as automating some processes, outsourcing some tasks, or prioritizing some data types or sources1, 2.

Question 3

Question Type: **MultipleChoice**

Your marketing team wants to know why they need a check box for their SMS opt-in. You explain it is part of the consumer's right to?

Options:

A- Request correction.

B- Raise complaints.

C- Have access.

D- Be informed.

Answer:

D

Explanation:

The marketing team needs a check box for their SMS opt-in because it is part of the consumer's right to be informed. This right means that consumers have the right to know how their personal data is collected, used, shared, and protected by the organization. The check box allows consumers to give their consent and opt-in to receive SMS messages from the organization, and also informs them of the purpose and scope of such messages. The other rights are not relevant in this case, as they are related to other aspects of data processing, such as correction, complaints, and access.Reference:CIPM Body of Knowledge, Domain IV: Privacy Program Communication, Section A: Communicating to Stakeholders, Subsection 1: Consumer Rights.

Question 4

Question Type: MultipleChoice

An online retailer detects an incident involving customer shopping history but no keys have been compromised. The Privacy Offce is most concerned when it also involves?

Options:

A- Internal unique personal identifiers.

B- Plain text personal identifiers.

C- Hashed mobile identifiers.

D- No personal identifiers.

Answer:

B

Explanation:

An online retailer detects an incident involving customer shopping history but no keys have been compromised. The Privacy Office is most concerned when it also involves plain text personal identifiers. Plain text personal identifiers are data elements that can directly identify an individual, such as name, email address, phone number, or social security number. Plain text means that the data is not encrypted or otherwise protected from unauthorized access or disclosure. If an incident involves plain text personal identifiers, it poses a high risk to the privacy and security of the customers, as their personal data could be exposed, stolen, misused, or manipulated by malicious actors. The Privacy Office should take immediate steps to contain, assess, notify, evaluate, and prevent such incidents,

.Reference:[CIPM - International Association of Privacy Professionals], [Free CIPM Study Guide - International Association of Privacy Professionals]

Question 5

Question Type: MultipleChoice

When conducting due diligence during an acquisition, what should a privacy professional avoid?

Options:

A- Discussing with the acquired company the type and scope of their data processing.

B- Allowing legal in both companies to handle the privacy laws and compliance.

C- Planning for impacts on the data processing operations post-acquisition.

D- Benchmarking the two Companies privacy policies against one another.

Answer:

B

Explanation:

When conducting due diligence during an acquisition, a privacy professional should avoid allowing legal in both companies to handle the privacy laws and compliance. This is because privacy is not only a legal issue, but also a business, technical, and operational issue that requires cross-functional collaboration and expertise. A privacy professional should be involved in the due diligence process to assess the privacy risks and opportunities of the acquisition, such as the type and scope of data processing, the data protection policies and practices, the data transfer mechanisms and agreements, the data breach history and response plans, and the impacts on the data processing operations post-acquisition. A privacy professional should also benchmark the two companies' privacy policies against one another to identify any gaps or inconsistencies that need to be addressed before or after the acquisition, .Reference:[CIPM - International Association of Privacy Professionals], [Free CIPM Study Guide - International Association of Privacy Professionals]

Question 6

Question Type: MultipleChoice

Under the General Data Protection Regulation (GDPR), what are the obligations of a processor that engages a sub-processor?

Options:

A- The processor must give the controller prior written notice and perform a preliminary audit of the sub-processor.

B- The processor must Obtain the controllers specifiC written authorization and provide annual reports on the sub-processor'S performance.

C- The processor must receive a written agreement that the sub-processor will be fully liable to the controller for the performance of its obligations in relation to the personal data concerned.

D- The processor must obtain the consent of the controller and ensure the sub-processor complies with data processing obligations that are equivalent to those that apply to the processor.

Answer:

D

Explanation:

Under the General Data Protection Regulation (GDPR), the obligations of a processor that engages a sub-processor are to obtain the consent of the controller and ensure the sub-processor complies with data processing obligations that are equivalent to those that apply to the processor. The GDPR defines a processor as a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller. A sub-processor is a third party that is engaged by the processor to carry out specific processing activities on behalf of the controller. The GDPR requires that the processor does not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorization, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. The processor must also ensure that the same data protection obligations as set out in the contract or other legal act between the controller and the processor are imposed on that other processor by way of a contract or other legal act under Union or Member State law, .Reference:[GDPR Article 28], [CIPM - International Association of Privacy Professionals]