DSCI
DCPLA
DSCI Certified Privacy Lead Assessor

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.2

Question: 1

_____ calls for inclusion of data protection from the onset of the designing of systems.

A. Agile Model
B. Privacy by Design
C. Logical Design
D. Safeguarding Approach

Answer: B

Explanation:
The concept of "Privacy by Design" is a core principle emphasized in the DSCI Privacy Framework (DPF©) and DSCI Assessment Framework for Privacy (DAF-P©). This principle requires that privacy be integrated into the design specifications and architecture of IT systems and business processes, right from the start of the development process rather than being added later as an afterthought.
The DSCI Privacy Framework states:
"Privacy by Design is a proactive approach that embeds privacy into the design and operation of IT systems, networked infrastructure, and business practices. It aims to ensure that privacy is built into the system by default, thereby preventing privacy-invasive events before they happen."
This ensures data protection is foundational to system architecture and not merely a compliance requirement added later. This proactive method mitigates risks and enhances user trust by safeguarding personal information through preventive measures rather than reactive ones.

Question: 2

Which of the following are classified as Sensitive Personal Data or Information under Section 43A of ITAA, 2008? (Choose all that apply.)

A. Password
B. Financial information
C. Sexual orientation
D. Caste and religious beliefs
E. Biometric information
F. Medical records and history

Answer: A, B, E, F

Explanation:
According to the DSCI Privacy Framework and as aligned with the Information Technology (Reasonable

Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, under Section 43A of the Information Technology Act, 2008, the following are considered Sensitive Personal Data or Information (SPDI):
Password Financial Information (such as bank account or credit card details)
Biometric Information (such as fingerprints, retina scans, etc.)
Medical Records and History
However, Sexual Orientation and Caste and Religious Beliefs are not explicitly included in the list of SPDI under Section 43A of the ITAA, 2008, though they may be protected under broader privacy considerations or sectoral regulations.
This classification helps in mandating appropriate security measures to protect such sensitive data, failure of which can result in compensation for damages to the affected individual due to negligence by the data processor or controller.

Question: 3

Entities should collect personal information from user that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This Privacy Principle is called:

A. Collection Limitation
B. Use Limitation
C. Accountability
D. Storage Limitation

Answer: A

Explanation:
According to the DSCI Privacy Framework and aligned with global privacy principles such as those found in the OECD and APEC frameworks, “Collection Limitation” emphasizes that personal data should be collected in a manner that is lawful and fair, and should be limited to what is necessary for the identified purposes.
As per DSCI Assessment Framework for Privacy (DAF-P©), this principle ensures organizations collect only relevant data by minimizing unnecessary data acquisition, thereby reducing the privacy risks. The principle mandates:
"Personal data collected should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed."
This is designed to promote responsible data stewardship and ensure minimal exposure of individuals’ personal information.

Question: 4

The method of personal data usage in which the users must explicitly decide not to participate.

A. Opt-In
B. Opt-out

C. Data mining
D. Data matching

Answer: B

Explanation:
The term “Opt-out” refers to a consent model in which individuals are automatically included in a data processing activity or program unless they explicitly indicate their desire not to participate.
Under the DSCI Privacy Framework, “Opt-out” is contrasted with “Opt-in,” where explicit affirmative consent is required before processing.
Opt-out is often implemented through mechanisms like pre-checked boxes or default settings, which the user can change. This is particularly common in direct marketing scenarios or cookies for analytics. The DAF-P© considers whether such consent mechanisms align with fairness and transparency principles.

Question: 5

An entity shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed; or with respect to an established retention period. This privacy principle is known as?

A. Collection Limitation
B. Use Limitation
C. Security safeguards
D. Storage Limitation

Answer: D

Explanation:
The “Storage Limitation” principle ensures that personal data is retained only for as long as necessary for the purposes for which it was collected.
The DSCI Privacy Framework and DAF-P© define this principle as:
"Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."
This prevents over-retention, minimizes risks of data breaches, and complies with legal and regulatory mandates for data minimization. Retention schedules and secure disposal practices are assessed under this principle in privacy audits.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/