Free Questions for DCPP-01 by actualtestdumps

Shared by Tillman on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following privacy legislations is synonymous with "Data Handlers"?

Options:

A- Federal Data Protection Act, Germany (BDSG)

B- South Korea's Personal Information Protection Act

C- Digital Privacy Act, 2015

D- Child online protection Act, 1998

Answer:

B

Question 2

Question Type: MultipleChoice

Specifically, what section of the IT (Amendment) Act, 2008 lays down the provisions for punishment for the offense of wrongful disclosure of personal information with the intention of causing loss or gain to another?

Options:

A- Section 72A

B- Section 65

C- Section 72

D- Section 43A

Answer:

D

Explanation:

There are two sections under the IT (Amendment) Act, 2008 that outline liabilities. These are quoted below: Sec 43A - "Where a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected." Compensation for failure to implement reasonable security practices can be upto Rs. 5 Crores (the Adjudicating Officer has the power to award this). A data subject can further approach a civil court if compensation desired is more than Rs. 5 Crore. Sec 72A - "Save as

otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both."

Question 3

Question Type: **MultipleChoice**

The Qatar Concerning Privacy and Protection of Personal Data Act, 2016 addresses different types of personal data, including:

Options:

A- Only manual processing of personal data

B- Only electronic processing of personal data

C- The electronic or manual processing of personal information

D- None of the above

Answer:

B

Explanation:

Page No 18 of PBok Addendum: The law is applicable to only personal data that is electronically processed or obtained, collected and extracted for electronic processing or when a combination of traditional and electronic processing is used. Following are situations where the law is not applicable: Any personal data (1) processed by individuals privately and when done in a family context & (2) gathered for official surveys and statistics The law is applicable to all residents of Qatar. It does not differentiate between Qataris and nonQataris.

Question 4

Question Type: MultipleChoice

Regarding projects such as Aadhaar, the National Population Register (NPR), etc. that involve national government projects specific to India, which of the following statements is accurate?

Options:

A- Citizens can choose not to submit their biometric details to the environment and can complete the process without providing their

biometrics

B- Prior to and during collection of data, data subjects are not properly notified

C- In India, biometric data collection is a statutory requirement

D- Once their personal information has been shared with the project, data subjects are not limited in how they can exercise control over how it will be used

Answer:

D

Explanation:

The requesting entity is expected to inform the individual, at the time of e-KYC authentication, what information will be shared with it by UIDAI on authentication and the purpose for which the information would be used. It is expected that notice is provided in the local language as well -- to ensure that the individual understands clearly what he/she is getting into. Any other entity other than the requesting entity that collects individual's Aadhaar number or even a document containing the Aadhaar number is also required to inform the individual the purpose of collection, whether it is mandatory and what are the alternatives. Consent After providing notice, the requesting entity is required to obtain the consent of the individual before collecting the identity information. The information may be collected in physical or, preferably, in electronic form. A record or log of the consent is also required to be maintained in the format specified by UIDAI. A requesting entity can do e-KYC authentication on behalf of a third party and share the e-KYC data with the third party for a specific purpose. However, it needs to take consent of the individual for this purpose. For any sharing of e-KYC data with a third party, a separate consent for each such sharing is required. The individual himself/herself may share their data with other entities. However, those entities cannot further share the data with any other entity without obtaining the individual's consent every single time it does a share. Similarly, any other entity other than the requesting entity that collects individual's Aadhaar number or any document

containing the Aadhaar number is also required to obtain the consent of the individual for the collection, storage and usage of the individual's Aadhaar number for the purpose specified. The individual has the freedom to revoke any of the earlier consent(s) given, and requesting entity would be required to delete e-KYC data along with ceasing its ability to share further. Usage and Purpose The requesting entity can use the identity information of an individual only for the purpose specified to the individual at the time of authentication or e-KYC. Similarly, any other entity other than the requesting entity that collects individual's Aadhaar number or any document containing the Aadhaar number can use the Aadhaar number only for those purposes specified to the individual at the time of obtaining his consent. Any other entity other than the requesting entity that collects individual's Aadhaar number or any document containing the Aadhaar number is not permitted to share the Aadhaar number with any other person without obtaining the consent of the individual. Disclosure The core biometric information collected under the Act is not allowed to be shared with anyone for any reason whatsoever. This is applicable to UIDAI as well as all agencies in the ecosystem. A requesting entity can share the identity data, including the e-KYC data, with third parties for any lawful purposes provided specific consent from the individual for the same has been obtained. However, the third party, in turn, cannot share it further with any other third party except to complete a transaction- that too only if the individual has given specific consent.

Question 5

Question Type: **MultipleChoice**

A growing economy has made it more important now than ever before for India to have comprehensive laws on _____.

Options:

A- Right to Information

B- Dispute resolution

C- Privacy

D- Right to Internet

Answer:

C

Explanation:

India has established privacy regime through a patchwork of legislations and regulations, unlike the European countries that have horizontal privacy laws. The Information Technology Act - IT Act 2000 -- was amended in 2008 to regulate privacy aspects and to provide assurance to customers that their privacy is protected through the use of 'reasonable security practices'. It achieved its purpose to some extent, but it does not satisfy all the requirements and expectations of a comprehensive privacy law. To address this, the Indian government is working on a comprehensive Privacy Protection Bill, which is likely to be based on Justice AP Shah Report, to which DSCI and NASSCOM have contributed as members.

Question 6

Question Type: MultipleChoice

Which of the following are needed for projects like DNA profiling, UIDAI, and statistical collection of individuals ?

Options:

A- Established a service which guarantees citizens' privacy only online

B- Protect the privacy of individuals

C- The need for a comprehensive privacy legislation at national level

D- None of the above

Answer:

C

Explanation:

Projects like UIDAI (Unique Identification Authority of India), NATGRID (National Intelligence Grid), CCTNS (Crime and Criminal Tracking Network and Systems), CMS (Central Monitoring System) etc in India are taking off -- which may have direct impact on privacy of individuals.This necessitates appropriate focus resultant legislations and regulatory measures for privacy to ensure safeguards and controls are put in place to support these kinds of projects.

Question 7

Question Type: MultipleChoice

According to RTI Act, under which conditions can a government department refuse to release information?

Options:

A- National security adversely affected by such information

B- This information is detrimental to the stability of the ruling party in government

C- Detrimental effect on the public image of government agencies

D- In the absence of a public interest, such information may adversely impact the privacy of its officials

Answer:

A, D

Question 8

Question Type: MultipleChoice

APPI, the Act for the Protection of Personal Information, applies to:

Options:

A- Government entities using personal information

B- Personal Information about an individual that is used by a business

C- None of the above

Answer:

B

Explanation:

The APPI is applicable to all businesses handling personal information for business use; however, national government, local governments and incorporated administrative agencies are excluded from the scope. The APPI is applicable to businesses in or outside Japan that collect personal information of Japanese citizens.

Question 9

Question Type: MultipleChoice

In the wake of privacy-related concerns arising from various policies around the world, which of the following has not driven increased regulatory responses?

Options:

A- Data privacy professionals are in high demand

B- Data flows across borders and outsourcing in a globalized world

C- Rapid growth of social networking sites, which are used to share a lot of personal information

D- Information about individuals having a greater economic value

Answer:

A

Explanation:

Rising demand of data privacy professionals is not concern.

Question 10

Question Type: MultipleChoice

Regulations that apply to the processing of personal data of natural persons that fall under the following categories:

Options:

A- EU Citizens

B- All of the above

C- Resident of anywhere in the world

D- EU Residents

Answer:

D

Explanation:

Page no 4 of PBok Addendum: The EU GDPR is applicable to all EU residents. The usage of the term 'residents' is to be noted -- it means that the resident need not be a citizen of any EU member state. It could be any individual who resides in the EU.

Question 11

Question Type: MultipleChoice

According to the EU, which of the following steps is not relevant when transferring data from an EU member to a third country that does not meet EU standards?

Options:

A- Obtaining approval by the Data Protection Authority or informing it

B- Aligning data protection legislation across geographies

C- Sizing up the security measures employed by the importing organization to account for the sensitivity of the data being transferred

D- A model contract is signed

Answer:

C

Question 12

Question Type: MultipleChoice

Choose from the options below to group privacy principles into user centric (requiring people's involvement) and organization centric (restricted to processes within the organization) categories:

Options:

A- User Centric: Choice, Collection Limitation, Access and Correction Organization Centric: Notice, Use Limitation, Security, Disclosure to third party, Accountability

B- User Centric: Notice, Consent, Collection Limitation, Access and Correction Organization Centric: Choice, Use Limitation, Security, Disclosure to third party, Openness, Accountability

C- User Centric: Notice, Openness, Accountability Organization Centric: Consent, Choice, Collection Limitation, Use Limitation, Security, Disclosure to third party, Access & Correction

D- User Centric: Notice, Consent, Choice, Access & Correction Organization Centric: Consent, Collection Limitation, Use Limitation, Security, Disclosure to third party, Openness, Accountability

Answer:

B

Explanation:

Page No 36 of PBok At a high level, Privacy Principles can be grouped into the following two categories: Principles that advocate user engagement: Principles such as Notice, Consent, Collection Limitation, Access & Correction etc. are user centric principles and involve

user transactions. Principles that are aligned to organizational context: Principles such as Purpose Limitation, Accountability, Disclosure, Security/Safeguard etc. talk about the norms and organizational measures for ensuring privacy protection by the organization.