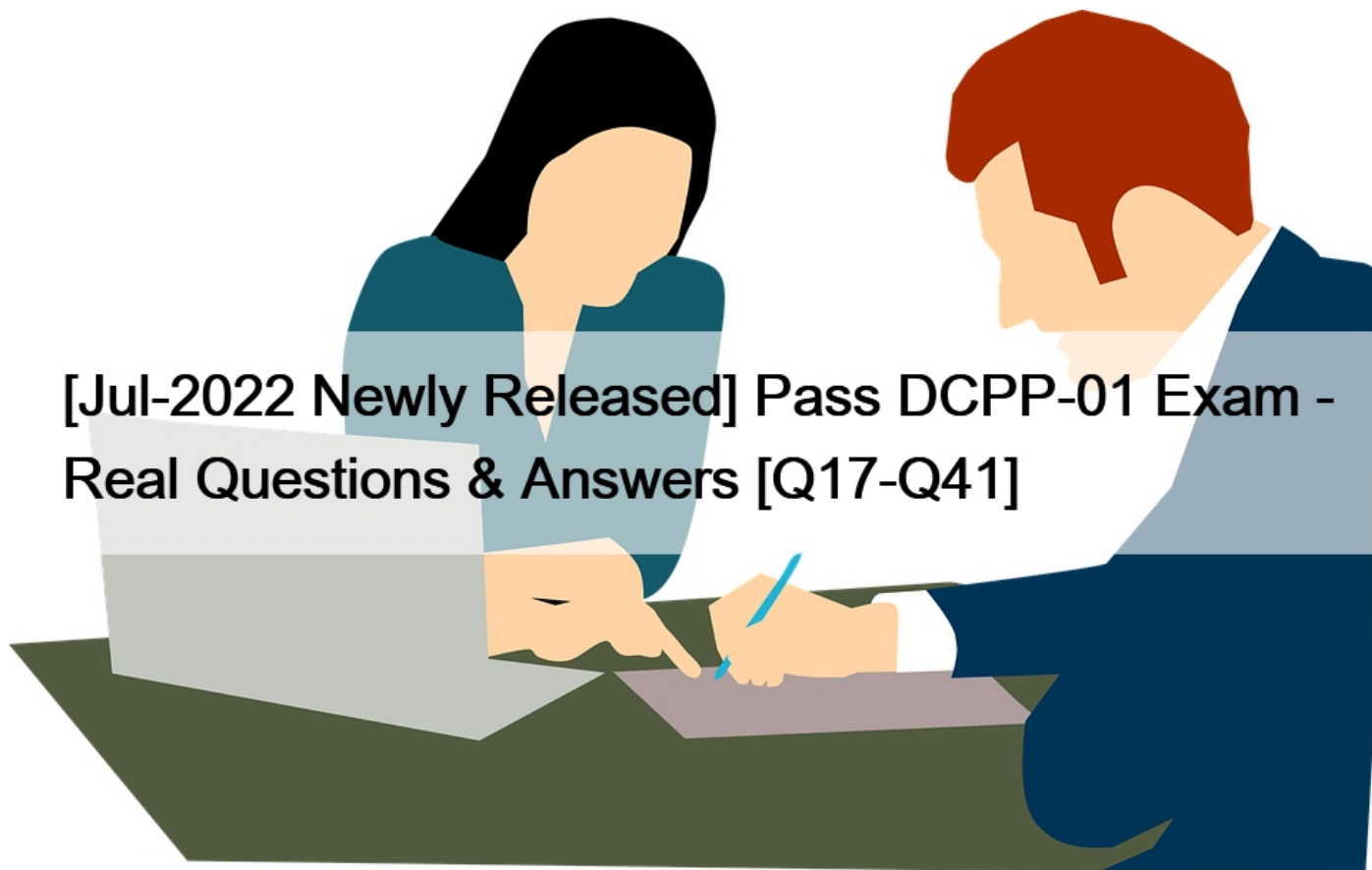


[Jul-2022 Newly Released Pass DCP-01 Exam - Real Questions & Answers [Q17-Q41]



[Jul-2022 Newly Released] Pass DCP-01 Exam - Real Questions and Answers
Pass DCP-01 Review Guide, Reliable DCP-01 Test Engine

What is the duration, language, and format of DSCI DCP-01 Privacy Professional Certification - Number of Questions: 65- Type of Questions: Multiple choice (MCQs), multiple answers- No negative marking for wrong answers- Duration of Exam: 130 minutes

How to Prepare For DSCI DCP-01 Privacy Professional Certification **Preparation Guide for DSCI DCP-01 Privacy Professional Certification Introduction for DSCI DCP-01 Privacy Professional Certification**

The accelerated rise of disruptive technologies & digitalization of services & transactions is exerting an impact on the working of the economy and society. This dependency on data to encourage businesses and reform have boosted potential hazards to the privacy of people. Various nations have tried to Mitigate this privacy risk through the implementation of administrative specifications, and responsibilities] to make businesses answerable for their actions.

Working under these laws becomes a significant hurdle faced by companies right from the initial stage of classification of the regulations that they are subjected to by virtue of the type of data they are dealing with and the extent of implementation of these laws, such as dealing with HIPAA compliance, or dealing with the effects of extraterritorial applicability of legislation such as the EU General Data Protection Regulation. There's a necessity for experts who are aware of the issues and impacts of data privacy to control privacy difficulties and risks.

Proficient privacy specialists are in demand, DCPD certification is what recruiters are seeking. When one achieves a DCPD credential, they earn the license to be acknowledged as part of a special group of competent and dedicated privacy specialists. DCPD is a pioneer credentialing program that enables individuals with expertise and equips them with the required skills to advance their career in the field of data privacy. It is an industry-standard certification for professionals joining and operating in the realm of privacy.

DSCI DCPD-01 Privacy Professional Certification course identifies a person's capability to establish and maintain the day-to-day data protection, monitoring, and privacy of a individuals to carry out particular corporate network security operations.

With 16,000+ active user certifications, the DCPD Privacy Expert certification program is earning notable industry attention. The value of the DCPD Privacy certification is verified every day by security specialists in the field and by trusted sources.

DSCI Certified Privacy course concentrates on the implementation and evaluation of a privacy program from a company's viewpoint, with a top focus on practice areas outlined in DPF. Comparing it with DCPD credentialing program, where the centre is on acquiring knowledge of privacy as a study field from a multi-dimension perspective. DCPD content is intended to help learners and working professionals learn different perspectives of privacy - general concepts, laws & regulations, privacy principles, tools and technologies etc., with a concise intro to privacy in an organizational environment- something that DCPLA examines into strongly. The two certifications are not linked. Hence, DCPLA applying for DCPD is entirely reliant on one's selection of what kind of expertise s/he wants to have in the Privacy domain.

All Privacy, Security and IT experts, Lawyers, Compliance Officers, Information System & Security Auditors, Risk Professionals and Students incorporated in Engineering, Law and Humanities in the final semester or have already graduated are encouraged to apply. This certification is recommended to them.

After finishing this course, the candidate will be able to:

- Offer an SSL VPN for secure access to a private network- Diagnose and repair common problems- Diagnose declined IKE exchanges- Execute a meshed or partially redundant VPN- Understand encryption uses and certificates- Propose DSCI DCPD-01 Single Sign-On access to network services, integrated with Microsoft Active Directory- Manage network access to configured networks using firewall policies- Partition FortiGate into two or more virtual devices, each operating as an autonomous FortiGate, by configuring virtual domains- Authorize an IPsec VPN tunnel connecting two FortiGate devices- Configure SD-WAN to load balance traffic amid multiple WAN links efficiently- Implement port forwarding, source NAT, and destination NAT- Recognize the features of the DSCI DCPD-01 Security Fabric- Stop hacking and denial of service (DoS) attacks- Utilize the GUI and CLI for management- Run packets using policy-based and static routes for multipath and load-balanced deployments- Deploy implicit and explicit proxy with firewall policies, authentication, and caching- Gather and understand log entries

Use **DSCI DCPD 01 practice exam** and **DSCI DCPD 01 practice exams** to prepare for the exam.

NEW QUESTION 17

For negligence in implementing and maintaining the reasonable security practices and procedures for

protecting Sensitive Personal Data or Information (SPDI) as mentioned in Section 43A and associated rules

under IT (Amendment) Act, 2008, a corporate entity may be liable to pay compensation of up to _____

- * Rs. 50,000,000
- * Rs. 500,000,000
- * Rs. 5,000,000
- * Upper limit not defined

Reference: <https://shodhganga.inflibnet.ac.in/bitstream/10603/164562/3/chapter%20ii.pdf>

NEW QUESTION 18

In relation to Online Privacy, please pick the incorrect statement:

- * Online disclosure of selective information by a person that is publicly available

- * The process of obtaining information online that a person can control
- * People's concerns over the license agreements they sign with any company
- * People's concern over the way their personal information is used during online activities

NEW QUESTION 19

According to IT (Amendment) Act, 2008, who should designate a grievance officer to redress grievance(s) of provider of information?

- * Data processor
- * Third party agency collecting personal information
- * Body corporate, which determines the means and purpose of data processing
- * Natural person sharing his/her information

Section: Privacy Principles and Laws

NEW QUESTION 20

Which of the following statement about Personally Identifiable Information (PII) is true?

- * PII is necessarily a single data element, not a combination of data elements, which can uniquely identify an individual
- * PII is a subset of Sensitive Personal Information
- * PII is any information about a legal entity including details of its registration or any information that may allow its easy identification
- * None of the above

Section: Privacy Fundamentals

NEW QUESTION 21

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?

- * Citizens can choose not to submit their biometric details to the environment and can complete the process without providing their biometrics
- * Prior to and during collection of data, data subjects are not properly notified
- * In India, biometric data collection is a statutory requirement
- * 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

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.

NEW QUESTION 22

A financial organization may share nonpublic information about its customers in accordance with Gramm-Leach-Bliley Act of the US. Which one of the following is the requirement?

- * Data sharing does not require consent from the consumers.
- * As soon as the GLBA privacy notice is disclosed initially and annually
- * FTC permission is required
- * Consumers's consent must be obtained first

NEW QUESTION 23

Among the following options, which would be the most appropriate for the transfer of Personal and Sensitive data from an EU company to another organization outside the EU?

- * The person transferring data to the destination country must inform the data protection commissioner, while the person exporting the data must notify the European Commission.
- * This case is not covered by the EU directive.
- * Putting in place suitable model contractual clauses is the vendor's responsibility in the third country.
- * A data exporter needs to create model contractual clauses after obtaining approvals from the data protection commissioner.

NEW QUESTION 24

You are part of a team that has been created by Indian government to create India's privacy law based on recommendations in Justice AP Shah's Report. Which of the following provisions should be addressed in the law?

- * Privacy as an explicit fundamental constitutional right
- * Offences, penalties and remedies
- * National privacy principles
- * Setup of a national data controller registry

NEW QUESTION 25

Which among the following can be classified as the most important purpose for enactment of data protection/ privacy regulations across the globe?

- * Protect the constitution
- * Penalize the organizations and impose fines for failure to protect privacy
- * Ensure peace in the society
- * Protect individual rights

NEW QUESTION 26

As a newly-appointed privacy officer of an IT company gearing up for DSCI's privacy certification, you are trying to understand what data elements are involved in each of the business process, function and if these data elements can be classified as sensitive personal information.

What is being accomplished with this effort?

- * Organization to get Visibility; over its exposure to sensitive personal information
- * It is a part of the annual exercise per the organization's privacy policy/ processes
- * Information security controls for confidential information being reviewed
- * Gathering inputs to restructure privacy function

Section: Privacy Technologies and Organization Ecosystem

NEW QUESTION 27

Rashmi recently started working as a customer care representative for a bank. After receiving a customer complaint over the phone, she wrote an email to send to grievance department in the bank. The email included customer's full name, bank account number, residential address, email address and contact number. She picked 2-3 resources/employees from the intranet site of the bank, which belonged to the grievance department and sent the email.

Please select the most ideal scenario from a privacy point of view?

- * Rashmi should have included some of the customer information in the email and send to grievance team.
- * Rashmi did the right thing by sharing all customer details to parties identified from company intranet.
- * Rashmi should have ascertained who in the grievance team is/are authorized to handle the complaint request and only then should have sent the customer details to the concerned person(s).
- * none of the above

Section: Privacy Fundamentals

NEW QUESTION 28

In India, who among the following would be the authorized legal entities to monitor and intercept communication of individuals?

- * Intermediaries; as defined under the IT (Amendment) Act, 2008
- * Telecom Service Providers
- * Intelligence and Law Enforcement Agencies
- * Directorate of Revenue Intelligence (DRI)

Section 69 Power to issue directions for interception or monitoring or decryption of any information through any computer resource.-(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

NEW QUESTION 29

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:

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

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

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

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.

NEW QUESTION 30

Which among the following organizations

- * WebTrust
- * Transaction Guard
- * BBBOnline
- * EuroPriSe

NEW QUESTION 31

A multinational company with operations in several parts within EU and outside EU, involves international data transfer of both its employees and customers. In some of its EU branches, which are relatively larger in size, the organization has a works council. Most of the data transferred is personal, and some of the data that the organization collects is sensitive in nature, the processing of some of which is also outsourced to its branches in Asian countries.

For the outsourced work of its customers' data processing, in order to initiate data transfer to another organizations outside EU, which is the most appropriate among the following?

- * The vendor (data importer) in the third country, and not the exporter is responsible to put in place suitable model contractual clauses, and hence the exporter does not need to take any action.
- * Since the data is processed by the vendor outside the EU, the EU directive does not apply and hence there are no legal concerns
- * The data exporter needs to initiate model contractual clauses after obtaining approvals from data protection commissioner and have the vendor be a signatory on the same as data importer
- * The data importer need to notify about the transfer to data protection commissioner in the destination country and exporter need to similarly notify in the EU country of origin

Section: Privacy Principles and Laws

NEW QUESTION 32

Which of the following could be considered as the most beneficial aspect of implementing Privacy Enhancing Technologies or Tools (PETs)?

- * Improves the quality of the information.
- * Reduces audit, supervisory and management costs.
- * Increases users' control over their personal data.
- * Ensures security by design in all products and services.

Section: Privacy Technologies and Organization Ecosystem

NEW QUESTION 33

Which of the following aspects of personal information lifecycle management should the privacy function in an organization be concerned with i. Policy definition ii. Policy enforcement iii. IT infrastructure setup iv. Physical infrastructure setup Please select the

correct option:

- * Only i.
- * Only i. and ii.
- * All
- * All except iv

Section: Privacy Technologies and Organization Ecosystem

Explanation/Reference:

NEW QUESTION 34

What are the roles an organization can play from privacy perspective?

- i. Data Controller – determines the means and purpose of processing of data which is collected from its end customers
- ii. Data Controller – determines the means and purpose of processing of data which is collected from its employees
- iii. Data Sub-Processor – processes personal data on behalf of data processor
- iv. Joint Controller – determines the means and purpose of data processing along with other data controller

Please select correct option:

- * i, ii and iii
- * ii, iii and iv
- * i, iii and iv
- * i, ii, iii and iv

NEW QUESTION 35

Which of the following laid foundation for the development of OECD privacy principles for the promotion of free international trade and trans border data flows?

- * Fair information Privacy Practices of US, 1974
- * EU Data Protection Directive
- * Safe Harbor Framework
- * WTO’s Free Trade Agreement

NEW QUESTION 36

‘Challenging Compliance’ as a privacy principle is covered in which of the following data protection/ privacy act?

- * Federal Data Protection Act, Germany
- * UK Data Protection Act
- * PIPEDA

- * Singapore Data Protection Act

NEW QUESTION 37

Effective 2013, HIPAA Omnibus rule applies to which of the following?

- * Covered Entities only
- * Business Associates only
- * Covered Entities & Business Associates
- * Federal Health Bodies only

The final Omnibus Rule becomes effective on March 26, 2013. Covered entities and Business Associates

NEW QUESTION 38

Which of the following parameters should ideally be addressed by a privacy program of an organization?

- * Privacy incident response plan and grievance handling
- * Environmental security concerns
- * Training and data classification
- * Intellectual Property (IP) protection

Section: Privacy Technologies and Organization Ecosystem

NEW QUESTION 39

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

- * EU Citizens
- * All of the above
- * Resident of anywhere in the world
- * EU Residents

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.

NEW QUESTION 40

Companies based in EU and willing to transfer data outside the EU/EEA, use model contracts as an instrument. Which of the following statements are true in reference to above statement?

- * It is a requirement mentioned in EU Data Protection Directive
- * It is a requirement mentioned in the OECD Privacy Framework
- * It is a requirement mentioned in the EU E-Commerce Directive
- * None of the above

NEW QUESTION 41

'Challenging Compliance' as a privacy principle is covered in which of the following data protection/ privacy act?

- * Federal Data Protection Act, Germany (BDSG)
- * UK Data Protection Act, 2018
- * Personal Information Protection and Electronic Documents Act (PIPEDA)
- * Singapore Data Protection Act, 2012

Section: Privacy Principles and Laws

100% Free DCP-01 Daily Practice Exam With 124 Questions: <https://www.vceprep.com/DCPP-01-latest-vce-prep.html>