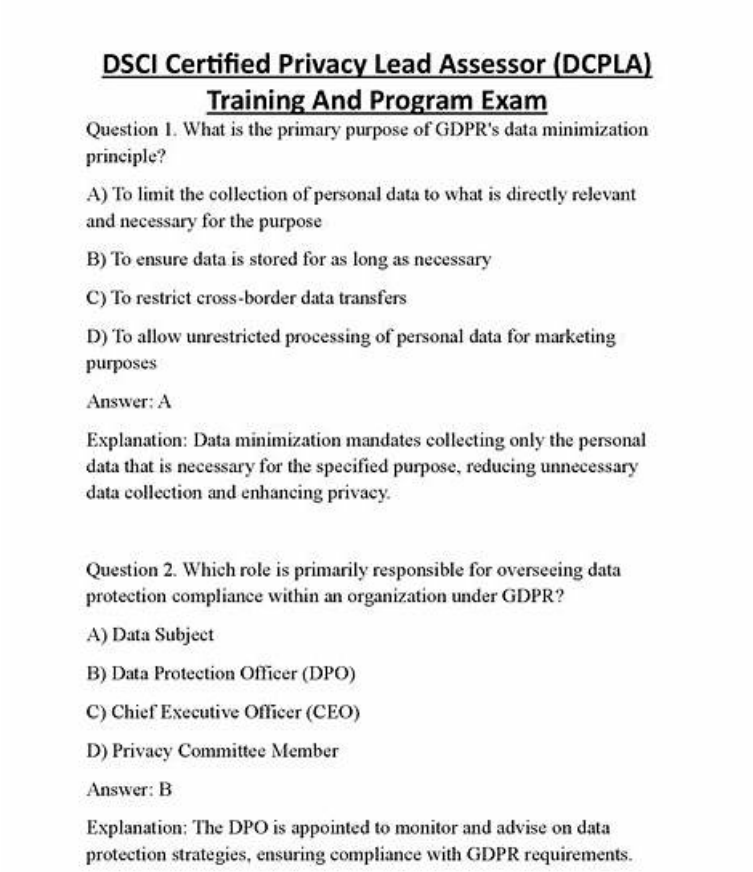
DSCI Certified Privacy Lead Assessor DCPLA certification Test Engine & DCPLA Free Pdf & DSCI Certified Privacy Lead Assessor DCPLA certification Actual Exam



DSCI Certified Privacy Lead Assessor (DCPLA) Training And Program Exam

Question 1. What is the primary purpose of GDPR's data minimization principle?

A) To limit the collection of personal data to what is directly relevant and necessary for the purpose

B) To ensure data is stored for as long as necessary

C) To restrict cross-border data transfers

D) To allow unrestricted processing of personal data for marketing purposes

Answer: A

Explanation: Data minimization mandates collecting only the personal data that is necessary for the specified purpose, reducing unnecessary data collection and enhancing privacy.

Question 2. Which role is primarily responsible for overseeing data protection compliance within an organization under GDPR?

A) Data Subject

B) Data Protection Officer (DPO)

C) Chief Executive Officer (CEO)

D) Privacy Committee Member

Answer: B

Explanation: The DPO is appointed to monitor and advise on data protection strategies, ensuring compliance with GDPR requirements.

2026 Latest ActualPDF DCPLA PDF Dumps and DCPLA Exam Engine Free Share: https://drive.google.com/open?id=1tBHwojshjwNBEM_G9HSILULFQ5chN1eR

In order to help these people who have bought the DCPLA study materials of our company, There is a team of expert in our company, which is responsible to renovate and update the DCPLA study materials provided by our company. We are going to promise that we will have a lasting and sustainable cooperation with customers who want to buy the DCPLA Study Materials from our company. If you decide to buy our DCPLA study materials, you will never miss any important information. In addition, we can promise the updating system is free for you.

The DCPLA certification exam is structured to evaluate a candidate's practical knowledge of privacy management frameworks, best practices, and legal requirements to help organizations implement and maintain effective privacy programs. DSCI Certified Privacy Lead Assessor DCPLA certification certification is aimed at professionals who are interested in developing their careers in the field of privacy management, including privacy officers, data protection officers, information security professionals, and compliance officers. DSCI Certified Privacy Lead Assessor DCPLA Certification certification exam is rigorous, and candidates must demonstrate their proficiency in privacy risk assessment, privacy compliance management, and privacy program management.

>> New DCPLA Test Topics <<

Prominent Features of DSCI DCPLA Exam Questions

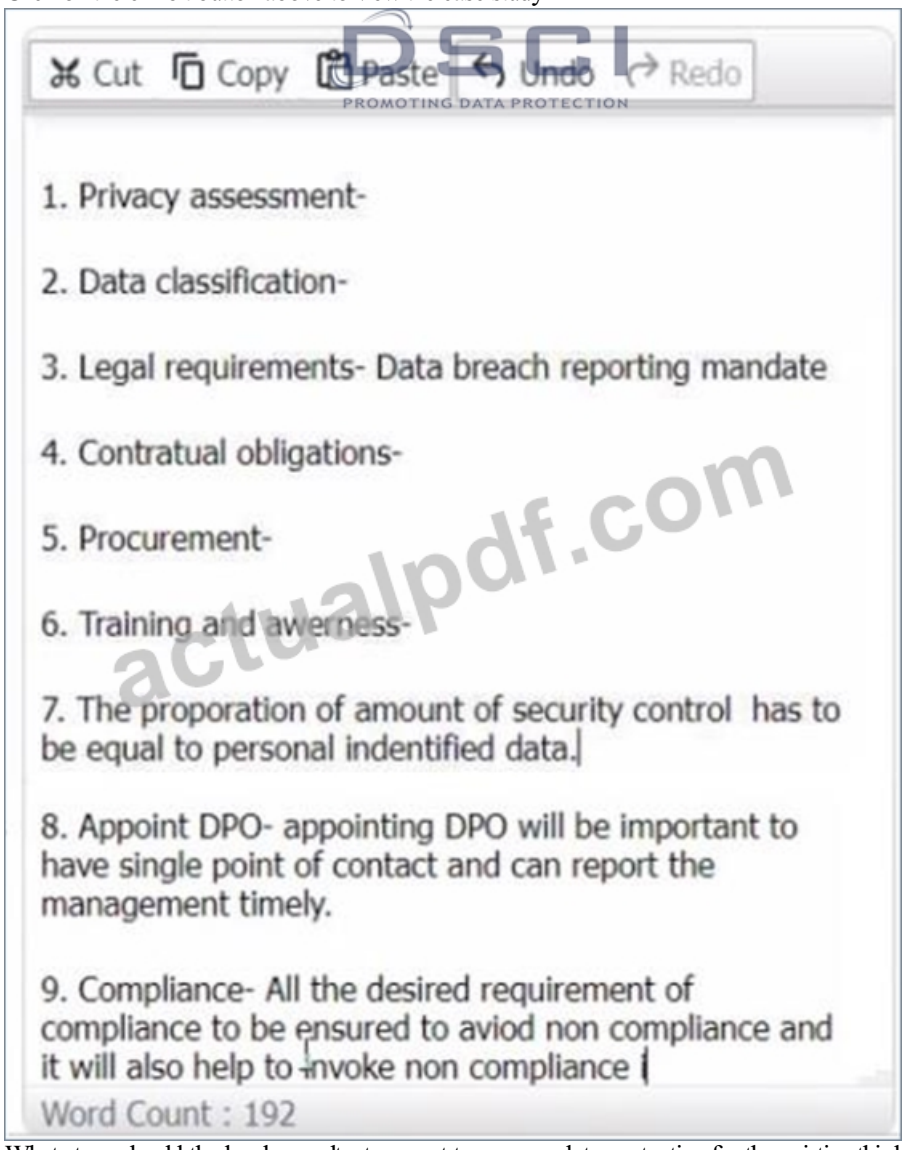
With pass rate reaching 98.75%, DCPLA exam torrent has received great popularity among candidates, and they think highly of the exam dumps. In addition, DCPLA exam braindumps are high-quality and accuracy, because we have professionals to verify the answers to ensure the accuracy. DCPLA exam dumps have most of knowledge points for the exam, and you can mater the major points through practicing. In addition, we have online and offline chat service for DCPLA Exam Dumps, and they posse the professional knowledge for the exam. If you have any questions about DCPLA exam materials, you can have a conversation with us.

The DCPLA certification exam covers a wide range of topics, including privacy laws and regulations, risk assessment and management, data protection strategies, and privacy impact assessment. DCPLA exam is designed to assess an individual's ability to evaluate and manage privacy risks, as well as their knowledge of best practices in privacy management. DCPLA Exam is rigorous and requires extensive preparation and study to pass.

DSCI Certified Privacy Lead Assessor DCPLA certification Sample Questions (Q98-Q103):

NEW QUESTION # 98
RCI and PCM
The Digital Personal Data protection Act 2023 has been passed recently. The Act shall be supported by subordinate Rules for various sections that will gradually bring more clarity into various aspects of the law.
First set of Rules are yet to be formulated and notified. A public sector bank has identified that it collects and processes personal data in physical documents and electronic form. The bank intends to assess its existing compliance level and proactively undertake an exercise to ensure compliance. Since this is the first time the bank is attempting to comply with a comprehensive privacy law, it has hired a legal expert in Privacy law to assist with initial assessment and compliance activities. As part of the initial visibility exercise the consultant identified that the bank collects and generates a significant amount of personal data in physical and digital form. The data may be upto 200 million customers' data. It is identified that customer onboarding is also done through various business correspondents in the field who collect and process personal data in physical and digital form on behalf of the bank for the purpose of opening bank accounts and this data is shared with the bank through various channels. There are upto 10 business correspondent companies that have been appointed by the bank across the country for such onboarding. These companies further appoint individual contractors on the field to face the customers. The legal consultant also identified that there are a huge number of employees and contractors engaged by the bank whose personal data is being collected and processed by the bank for HR purposes including biometric based attendance. While the intent of initial assessment was the new Act, the legal consultant has also identified that the Bank collects Aadhaar numbers (voluntary submission) from customers and employees and may be subject to Aadhaar Act compliance. It also came as a surprise that the bank wasn't aware of the data breach reporting mandate by one of the regulatory bodies under the Information Technology Act 2000 and that it was a criminal offense. The Bank generally outsources all non-core activities such as call centers which are handled by an Indian BPO company and document warehousing which is handled by another company. The Bank has also moved many of its applications to a known cloud provider as part of its digital strategy and there may be data transfer aspects associated with the same. On review of various contracts with third parties it was identified that the bank has signed standard terms of the cloud provider and has signed contracts with third parties which were in standard format of the third parties. Data protection obligations are not clear or available in these contracts. Bank leadership has been of the opinion that even the third parties should comply with the laws and robust contracts on legal compliance may not be needed. The legal consultant is not just expected to help identify gaps. assist in fixing the gaps but also to help implement controls and processes to continuously comply with evolving Rules under the new Act and also manage data protection with various third parties that may be appointed in the future.
(Note: Candidates are requested to make and state assumptions wherever appropriate to reach a definitive conclusion) Introduction and Background XYZ is a major India based IT and Business Process Management (BPM) service provider listed at BSE and NSE. It has more than 1.5 lakh employees operating in 100 offices across 30 countries. It serves more than
500 clients across industry verticals - BFSI, Retail, Government, Healthcare, Telecom among others in Americas, Europe, Asia-Pacific, Middle East and Africa. The company provides IT services including application development and maintenance, IT Infrastructure management, consulting, among others. It also offers IT products mainly for its BFSI customers.
The company is witnessing phenomenal growth in the BPM services over last few years including Finance and Accounting including credit card processing, Payroll processing, Customer support, Legal Process Outsourcing, among others and has rolled out platform based services. Most of the company's revenue comes from the US from the BFSI sector. In order to diversify its portfolio, the company is looking to expand its operations in Europe. India, too has attracted company's attention given the phenomenal increase in domestic IT spend esp. by the government through various large scale IT projects. The company is also very aggressive in the cloud and mobility space, with a strong focus on delivery of cloud services. When it comes to expanding operations in Europe, company is facing difficulties in realizing the full potential of the market because of privacy related concerns of the clients arising from the stringent regulatory requirements based on EU General Data Protection Regulation (EU GDPR).
To get better access to this market, the company decided to invest in privacy, so that it is able to provide increased assurance to potential clients in the EU and this will also benefit its US operations because privacy concerns are also on rise in the US. It will also

help company leverage outsourcing opportunities in the Healthcare sector in the US which would involve protection of sensitive medical records of the US citizens.
The company believes that privacy will also be a key differentiator in the cloud business going forward. In short, privacy was taken up as a strategic initiative in the company in early 2011.
Since XYZ had an internal consulting arm, it assigned the responsibility of designing and implementing an enterprise wide privacy program to the consulting arm. The consulting arm had very good expertise in information security consulting but had limited expertise in the privacy domain. The project was to be driven by CIO's office, in close consultation with the Corporate Information Security and Legal functions.
Click on the exhibit button above to view the case study



What steps should the legal consultant suggest to manage data protection for the existing third parties with whom there are existing contracts? Please also mention the various controls that should be implemented with these third parties to ensure continued compliance and monitoring Please answer with respect to the PCM practice area (upto 250 words)

Answer:

Explanation:
See the answer below in explanation.
Explanation:
To manage data protection risks associated with third-party engagements, the legal consultant should take a structured Privacy Contract Management (PCM) approach. This involves:
* Conduct a comprehensive review of all third-party contracts (e.g., cloud provider, BPO, document warehouse, business correspondents).
* Identify gaps related to privacy and data protection clauses (which are currently unclear or missing).
* Categorize vendors based on risk level (data sensitivity, volume, criticality, location).
1. Contract Review & Risk Categorization:
2. Define Privacy Obligations in Contracts:Update or re-negotiate contracts to include:

* Data Processing Clauses: Clearly outline roles (Data Fiduciary vs. Processor), purpose limitation, retention policies.
* Breach Notification: Mandate immediate reporting of data breaches by vendors (as per IT Act & upcoming DPDP Rules).
* Aadhaar Handling: For any third-party collecting Aadhaar, add compliance clauses for Aadhaar Act.
* Cross-border Transfers: Ensure compliance with Section 16 of DPDP Act, if data leaves India (e.g., via cloud provider).
* Audit Rights: Include rights to audit vendor privacy practices and security controls.
* Establish Third-Party Risk Assessments (TPRA) and due diligence during onboarding and periodically.
* Mandate privacy training for third-party staff handling personal data.
* Enforce technical and organizational controls: Encryption, access control, secure transmission.
* Implement a Vendor Monitoring Framework - regular privacy compliance checks, reporting, and corrective action tracking.
3. Implement Ongoing Controls:
* Assign a Third-Party Privacy Officer or include the DPO in oversight.
* Maintain a Third-Party Data Processing Register (as required under DPDP Act).
4. Governance and Reporting:

NEW QUESTION # 99
In the landmark case _____ the Honourable Supreme Court of India reaffirmed the status of Right to Privacy as a Fundamental Right under Part III of the constitution.

- A. Olga Tellis vs. Bombay Municipal Corporation
- B. M. P. Sharma and others vs. Satish Chandra, District Magistrate, Delhi, and others
- C. Justice K. S. Puttaswamy (Retd.) and Anr. vs. Union of India And Ors
- D. Maneka Gandhi vs. Union of India

Answer: C

NEW QUESTION # 100
What are the two phases of DSCI Privacy Third Party Assessment?

- A. Primary and Secondary
- B. Initial and Final
- C. None of the above
- D. Initial and Detailed

Answer: D

Explanation:
The DSCI Assessment Framework for Privacy (DAF#P) outlines that the Privacy Third Party Assessment is conducted in two phases:
* Initial Assessment - High-level review of privacy practices and process readiness
* Detailed Assessment - In-depth evaluation of privacy implementation and evidence review This phased approach allows assessors to identify maturity gaps early and gather comprehensive evidence in the second phase.

NEW QUESTION # 101
Which of the following wasn't prescribed as a privacy principle under the OECD Privacy Guidelines, 1980?

- A. Openness
- B. Data Minimization
- C. Security Safeguard
- D. Purpose Specification

Answer: B

Explanation:
The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) defined eight core privacy principles:
* Collection Limitation
* Data Quality
* Purpose Specification

* Use Limitation
* Security Safeguards
* Openness
* Individual Participation
* Accountability

"Data Minimization" was not part of the original 1980 OECD principles. While it is a common privacy principle today and included in modern frameworks like GDPR and DSCI's DPF, it was not part of the original OECD set.

NEW QUESTION # 102

FILL BLANK

RCI and PCM

Given its global operations, the company is exposed to multiple regulations (privacy related) across the globe and needs to comply mostly through contracts for client relationships and directly for business functions. The corporate legal team is responsible for managing the contracts and understanding, interpreting and translating the legal requirements. There is no formal tracking of regulations done. The knowledge about regulations mainly comes through interaction with the client team. In most of the contracts, the clients have simply referred to the applicable legislations without going any further in terms of their applicability and impact on the company. Since business expansion is the priority, the contracts have been signed by the company without fully understanding their applicability and impact. Incidentally, when the privacy initiatives were being rolled out, a major data breach occurred at one of the healthcare clients located in the US. The US state data protection legislation required the client to notify the data breach. During investigations, it emerged that the data breach happened because of some vulnerability in the system owned by the client but managed by the company and the breach actually happened 5 months back and came to notice now. The system was used to maintain medical records of the patients. This vulnerability had been earlier identified by a third party vulnerability assessment of the system and the closure of vulnerability was assigned to the company. The company had made the requisite changes and informed the client. The client, however, was of the view that the changes were actually not made by the company and they therefore violated the terms of contract which stated that - "the company shall deploy appropriate organizational and technology measures for protection of personal information in compliance with the XX state data protection legislation." The company could not produce necessary evidences to prove that the configuration changes were actually made by it (including when these were made).

(Note: Candidates are requested to make and state assumptions wherever appropriate to reach a definitive conclusion) Introduction and Background XYZ is a major India based IT and Business Process Management (BPM) service provider listed at BSE and NSE. It has more than 1.5 lakh employees operating in 100 offices across 30 countries. It serves more than 500 clients across industry verticals - BFSI, Retail, Government, Healthcare, Telecom among others in Americas, Europe, Asia-Pacific, Middle East and Africa. The company provides IT services including application development and maintenance, IT Infrastructure management, consulting, among others. It also offers IT products mainly for its BFSI customers.

The company is witnessing phenomenal growth in the BPM services over last few years including Finance & Accounting including credit card processing, Payroll processing, Customer support, Legal Process Outsourcing, among others and has rolled out platform based services. Most of the company's revenue comes from the US from the BFSI sector. In order to diversify its portfolio, the company is looking to expand its operations in Europe. India, too has attracted company's attention given the phenomenal increase in domestic IT spend esp. by the government through various large scale IT projects. The company is also very aggressive in the cloud and mobility space, with a strong focus on delivery of cloud services. When it comes to expanding operations in Europe, company is facing difficulties in realizing the full potential of the market because of privacy related concerns of the clients arising from the stringent regulatory requirements based on EU General Data Protection Regulation (EU GDPR).

To get better access to this market, the company decided to invest in privacy, so that it is able to provide increased assurance to potential clients in the EU and this will also benefit its US operations because privacy concerns are also on rise in the US. It will also help company leverage outsourcing opportunities in the Healthcare sector in the US which would involve protection of sensitive medical records of the US citizens.

The company believes that privacy will also be a key differentiator in the cloud business going forward. In short, privacy was taken up as a strategic initiative in the company in early 2011.

Since XYZ had an internal consulting arm, it assigned the responsibility of designing and implementing an enterprise wide privacy program to the consulting arm. The consulting arm had very good expertise in information security consulting but had limited expertise in the privacy domain. The project was to be driven by CIO's office, in close consultation with the Corporate Information Security and Legal functions.

What should be the learning for the company going forward? What should the consultants suggest? (250 to 500 words)

Answer:

Explanation:

The consultants should suggest a comprehensive and integrated privacy program for the company which addresses the current regulatory requirements while being proactive in anticipating any changes to these regulations. The program should be effective, flexible, cost-efficient and easy to understand & implement.

To begin with, the program should involve an assessment of all existing processes and procedures that are related to personal data processing in order to identify potential areas of risk. The potential risks along with recommended mitigating controls should then be documented in a Privacy Impact Assessment (PIA) report.
This will enable the organization to assess its compliance level against applicable regulations.
It is also important for XYZ to have strong Data Governance policies & procedures along with appropriate organizational structures and accountability mechanisms in place. This will include a Data Privacy Officer (DPO) who is responsible for overseeing the compliance program and being the point of contact for data protection supervisory authorities. The DPO should be part of the management team and report to the CIO's office as well as senior-level executives.
A consultant should also recommend data minimization, pseudonymization, encryption, and other security measures to protect personal information. In addition, they can recommend regular privacy awareness training sessions for employees, so that they are up-to-date on changes in regulations and understand how their role impacts data privacy and security. Lastly, all systems & processes should be monitored & audited to ensure compliance with relevant regulations.
As a result, consultants should provide clients in the EU and US with an integrated & comprehensive privacy program that provides the necessary assurances and protects sensitive data from unauthorized access or misuse. By leveraging outsourcing opportunities in the healthcare sector in the US, XYZ could potentially gain competitive advantage.

NEW QUESTION # 103
.....