# DCPLA Q&As

DSCI Certified Privacy Lead Assessor DCPLA certification

## Pass DSCI DCPLA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.pass4itsure.com/dcpla.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by DSCI Official Exam Center

**QUESTION 1**

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. M. P. Sharma and others vs. Satish Chandra, District Magistrate, Delhi, and others

B. Maneka Gandhi vs. Union of India

C. Justice K. S. Puttaswamy (Retd.) and Anr. vs. Union of India And Ors

D. Olga Tellis vs. Bombay Municipal Corporation

Correct Answer: C

**QUESTION 2**

Categorize the following statements as: Visibility/ Capability /Enforcement /Demonstration Problems

"The network is unable to restrict unwanted external connections carrying sensitive information."

A. Visibility

B. Capability

C. Enforcement

D. Demonstration

Correct Answer: B

**QUESTION 3**

The assessor organization can issue the DSCI certification to the assessee organization if it is satisfied with the assessment outcome.

A. True

B. False

Correct Answer: A

**QUESTION 4**

Following aspects can serve as inputs to a privacy organization for ensuring privacy protection:

I) Privacy related incidents detected/reported

II) Contractual obligations

III) Organization\\'s exposure to personal information

IV) Regulatory requirements

A. I, II and III

B. II and IV

C. I, II, III and IV

D. None of the above, as privacy and compliance protection mechanisms are evolved based only on organization\\'s privacy policies and procedures

Correct Answer: C

**QUESTION 5**

PPP

Based on the visibility exercise, the consultants created a single privacy policy applicable to all the client relationships and business functions. The policy detailed out what PI company deals with, how it is used, what security measures are deployed for protection, to whom it is shared, etc. Given the need to address all the client relationships and business functions, through a single policy, the privacy policy became very lengthy and complex. The privacy policy was published on company\\'s intranet and also circulated to heads of all the relationships and functions. W.r.t. some client relationships, there was also confusion whether the privacy policy should be notified to the end customers of the clients as the company was directly collecting PI as part of the delivery of BPM services. The heads found it difficult to understand the policy (as they could not directly relate to it) and what actions they need to perform. To assuage their concerns, a training workshop was conducted for 1 day. All the relationship and function heads attended the training.

However, the training could not be completed in the given time, as there were numerous questions from the audiences and it took lot of time to clarify.

(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.

Do you agree with company\\'s decision to have single privacy policy for all the relationships and functions? Please justify your view. (250 to 500 words)

A. See the answer in explanation below.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

Yes, I agree with the company\\'s decision to have a single privacy policy for all its relationships and functions. Having a unified privacy policy allows the organization to communicate consistently across multiple channels of communication with

customers, partners and vendors. It also ensures that all stakeholders are aware of their rights when dealing with personal data and makes it easier for them to understand their responsibilities when handling such information.

Moreover, having a standardized privacy policy helps to protect the company from potential legal repercussions due to inadequate protection of confidential data. The need for comprehensive protection is especially important in this age

where cyber-attacks are becoming increasingly frequent and sophisticated. By putting in place a consistent framework that governs how any organization handles sensitive information can help reduce the risks associated with data breaches.

By demonstrating that the company takes strong measures to protect its customers\\' personal information, a single privacy policy can help boost the company\\'s reputation and build trust with customers. Compliance with a variety of regulatory

requirements is especially important for companies operating in regulated industries, such as banking and healthcare.

In addition, having a unified privacy policy allows organizations to maintain control over how their data is stored and processed. By monitoring who has access to confidential information, companies can identify any potential security

vulnerabilities before they are exploited by malicious actors.

To conclude, I support XYZ\\'s decision to have one privacy policy for all its relationships and functions. Having a unified privacy policy can help the organization protect itself from potential legal risks, boost its reputation and maintain control

over how data is stored and used. All in all, it is an important step to ensure that customer data is always kept safe and secure.

**QUESTION 6**

There are several privacy incidents reported in an organization. The organization plans to analyze and learn from these incidents. Which privacy practice will the organization have to implement for the same?

A. Information usage and access

B. Privacy contract management

C. Privacy awareness and training

D. Privacy monitoring and incident management

Correct Answer: D

**QUESTION 7**

An organization is always a data controller for its _____.

A. Employees

B. Client

C. Supervisory authority

D. None of the above

Correct Answer: A

**QUESTION 8**

Arrange the following techniques in decreasing order of the risk of re-identification:

I) Pseudonymization II) De-identification III) Anonymization

A. I, II

B. III, II, I

C. II, III, I

D. All have equal risk of re-identification

Correct Answer: C

**QUESTION 9**

Which of the following is not an objective of POR?

A. Create an inventory of business processes, enterprise and operational functions, client relationships that deal with personal information

B. Identify all the activities, functions and operations that can be attributed to the privacy initiatives of an organization

C. Evaluate the role of corporate function in legal compliance management, its relations with IT, and security functions. Evaluate the role of legal function in compliance matters

D. Establish a privacy function to address the activities, functions and operations that are required to manage the privacy initiatives

Correct Answer: C

**QUESTION 10**

Privacy enhancing tools aim to allow users to take one or more of the following actions related to their personal data that is sent to, and used by online service providers, merchants or other users:

I) Increase control over their personal data

II) Choose whether to use services anonymously or not

III) Obtain informed consent about sharing their personal data

IV) Opt-out of behavioral advertising or any other use of data

A. Only I

B. Only I and II

C. I, II, III and IV

D. Only II

Correct Answer: C

**QUESTION 11**

_____ 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

Correct Answer: B

**QUESTION 12**

IUA and PAT

The company has a very mature enterprise level access control policy to restrict access to information. There is a single sign-on platform available to access company resources such as email, intranet, servers, etc. However, the access policy in client relationships varies depending on the client requirements. In fact, in many cases clients provide access ids to the employees of the company and manage them. Some clients also put technical controls to limit access to information such data masking tool, encryption, and anonymizing data, among others. Some clients also record the data collection process to monitor if the employee of the company does not collect more data than is required. Taking cue from the best practices implemented by the clients, the company, through the consultants, thought of realigning its access control policy to include control on data collection and data usage by the business functions and associated third parties. As a first step, the consultants advised the company to start monitoring the PI collection, usage and access by business functions without their knowledge. The IT function was given the responsibility to do the monitoring, as majority of the information was handled electronically. The analysis showed that many times, more information than necessary was collected by the some functions, however, no instances of misuse could be identified. After few days of this exercise, a complaint was registered by a female company employee in the HR function against a male employee in IT support function. The female employee accused the male employee of accessing her photographs stored on a shared drive and posting it on a social networking site.

(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.

What should the company do to limit data collection and usage and at the same time ensure that such kinds of incidents don\\'t reoccur? (250 to 500 words)

A. See the answer in explanation below.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

XYZ should strive to create a comprehensive privacy policy that addresses all aspects of data collection, usage and storage. This will both protect the company from legal liabilities as well as create an environment of trust between customers and the organization. It should also ensure that proper security controls are in place for both on-premise systems as well as cloud services. The policy should outline details regarding access privileges and procedures for handling sensitive personal information including photographs. Further, XYZ should conduct regular training sessions with employees, especially those in IT support functions, to enhance their knowledge about the company\\'s privacy policies and procedures. An employee code of conduct outlining restrictions on the misuse of data must be implemented and communicated clearly to all stakeholders involved in data processing activities. The company should also implement technical measures such as encryption and pseudonymisation of data, which will ensure that the data is only accessible by authorized personnel with proper privileges. In addition to this, XYZ should also create a framework for breach notification that outlines the steps to be taken in case of any unauthorized access or disclosure of information. The policy should set out procedures for assessing incidents and for informing the relevant authorities as well as affected individuals within a specified timeframe. Finally, XYZ should develop an independent monitoring mechanism to ensure compliance with its privacy policies and procedures. This may include third-party audits, regular evaluation of existing policies, and periodic reviews of employee performance. By investing in privacy and security controls at both procedural and technical levels, XYZ can ensure that it is able to keep pace with the ever-evolving privacy landscape and provide its customers with the assurance they need. This will also help the company meet any new regulatory requirements as well as ensure that similar incidents don\\'t reoccur in the future. In this way, XYZ will be able to successfully access and tap into potential markets while reducing legal liabilities associated with data misuse. The bottom line is that proper investment in privacy and security will yield long-term dividends by enhancing customer trust in the organization. By implementing a comprehensive framework of policies, procedures and technical measures, XYZ can protect personal information from unauthorized access or disclosure, thereby providing increased assurance to customers that their data is safe and secure. In this way, the company will be better positioned to remain competitive in an increasingly competitive landscape.

**QUESTION 13**

Which of the following best describes `Processing\\'?

A. Processing is collection and use of personal data

B. Processing is storage and structuring personal data

C. Processing is recording and destruction of personal data

D. Processing is a blanket term used for the wide range of operations performed on personal data

Correct Answer: B

**QUESTION 14**

What is the maximum compensation that can be imposed on an organization for negligence in implementing reasonable security practices as defined in Section 43A of ITAA, 2008?

A. Uncapped compensation

B. 5 crores

C. 15 crores or 4% of the global turnover

D. 5 lakhs

Correct Answer: C

**QUESTION 15**

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 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.

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

A. See the answer in explanation below.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

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 and 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 and 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 and processes should be monitored and audited to ensure compliance with relevant regulations. As a result, consultants should provide clients in the EU and US with an integrated and 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.