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.leads4pass.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

Which of the following are the key factors that need to be considered for determining the applicability of the privacy principles? (Choose all that apply.)

A. The role of the organization in determining the purpose of the data collection

B. How and where the data is coming in the organization

C. Requirements stipulated by the local authorities from where the organization operating

D. Organization\\'s commitment to the external stakeholder with respect to privacy

Correct Answer: AB

QUESTION 2

Which of the following mechanisms can be used to transfer personal data outside of a country?

A. Binding corporate rules

B. Adequacy decision

C. Standard contractual clauses

D. All of the above

Correct Answer: D

QUESTION 3

Which of the following wasn\\'t prescribed as a privacy principle under the OECD Privacy Guidelines, 1980?

A. Openness

B. Security Safeguard

C. Data Minimization

D. Purpose Specification

Correct Answer: A

QUESTION 4

Which of the following does the `Privacy Strategy and Processes\\' layer in the DPF help accomplish? (Choose all that apply.)

A. Visibility over Personal Information

B. Privacy Policy and Processes

C. Regulatory Compliance Intelligence

D. Information Usage and Access

E. Personal Information Security

Correct Answer: ABDE

QUESTION 5

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.

Why do you think the company failed to defend itself against client accusations? (250 to 500 words)

A. See the answer in explanation below.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

The company failed to defend itself against accusations by its clients most likely due to the fact that it did not have enough expertise in privacy and data protection. The company\\'s privacy program was designed and implemented by an internal consulting arm which had limited expertise in the domain, causing the program to be inadequate for the purpose of defending itself against accusations. Moreover, since the project was driven by CIO\\'s office, there may have been a lack of coordination between different functions like Corporate Information Security and Legal functions which could also have contributed to the failure. It is possible that there were gaps in the organizational measures deployed by XYZ as well as gaps in technology measures. For example, it is possible that although appropriate organizational measures were put in place, the technology measures were inadequate for protecting the sensitive data of its clients. In addition, it is possible that the company did not rigorously monitor compliance with these organizational and technological measures, thereby making it vulnerable to accusations by its clients. It is also likely that XYZ was unable to fully comply with applicable privacy laws and regulations in the EU due to lack of awareness about their requirements as well as insufficient resources allocated for adapting to them. The EU GDPR requires companies to implement appropriate technical and organizational measures for the protection of personal data which could have been a challenge for XYZ given its limited expertise in this domain. Furthermore, even though it may have had some understanding of the legal requirements, there may have been difficulty in properly implementing them, which could have led to the accusations by its clients. Finally, it is possible that XYZ failed to defend itself against client accusations because of a lack of communication between its different departments and functions. The company may not have had a clear understanding of the requirements and risks associated with data protection and privacy compliance which could have caused miscommunication among various stakeholders leading to inadequate responses when it was challenged by its clients. Overall this case study demonstrates the importance of properly designing and implementing an effective privacy program in order to protect sensitive data from unauthorized access or misuse. Companies should ensure that they have adequate expertise in data protection as well as sufficient resources for adapting to changing regulatory requirements in order to avoid potential legal issues arising from client accusations. Effective communication and coordination across different departments and functions is also essential for successful data protection compliance. It is recommended that companies invest in an ongoing training program to ensure that employees understand the importance of privacy, have an awareness of the legal requirements, and are able to properly implement security measures to protect sensitive data. Organizations should also consider implementing automated tools and technologies such as encryption, access control systems, identity management solutions, etc., which can help them better defend themselves against potential client accusations.

QUESTION 6

Create an inventory of the specific contractual terms that explicitly mention the data protection requirements. This an imperative of which DPF practice area?

A. Visibility over Personal Information (VPI)

B. Information Usage and Access (IUA)

C. Privacy Contract Management (PCM)

D. Regulatory Compliance Intelligence (RCI)

Correct Answer: C

QUESTION 7

RCI and PCM

In April 2011, the rules were issued under Section 43A of the IT Act by the Government of India and the `body corporates\\' were required to comply with these rules. The Corporate legal team tried to understand and interpret the rules but struggled to understand its applicability esp. to client relationships and business functions. So, the company hired an IT Act legal expert to advise them on the Section 43A rules.

To start with, the company identified the PI dealt with by business functions as part of the earlier visibility exercise, but it wanted to reassure itself. Therefore, a specific exercise was conducted to revisit `sensitive personal information\\' dealt by business functions. It was realized that the company collects lot of SPI of its employees and therefore `reasonable security practices\\' need to be adhered to by the functions that deal with SPI. It was also ascertained that many of this SPI is being dealt by third parties, some of which are also located outside India. To meet the requirements of the rules, the company reviewed all the contracts and inserted a clause ?`the service provider shall implement reasonable security practices and procedures as per the IT (Amendment) Act, 2008\\'. Some of the large service providers were ISO 27001 certified and they claimed that they fulfill the requirements of `reasonable security practices\\'. However, some SME service providers did not understand what would `reasonable security practices\\' imply and requested the company to clarify, which referred them to Rule 8 of the Section 43A. Some small scale service providers expressed their unwillingness to get ISO certified, given the costs involved.

(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.

Did the company take sufficient steps to protect SPI dealt by its service providers and ensure that it complies with the regulatory requirements? Was referring to `reasonable security practices\\' sufficient in the contracts or the company should have also considered some other measures for privacy protection as well? (250 to 500 words)

A. See the answer in explanation below.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

The consulting arm of XYZ developed a comprehensive privacy program in line with the company\\'s goal to leverage its existing technology infrastructure, resources and capabilities for protecting data. The program had three parts ? awareness and training, policy development and implementation. On the awareness front, extensive training was conducted for employees on various aspects of privacy including GDPR compliance. This was followed by the development and rollout of an enterprise-wide privacy policy which clearly defined the various steps to be taken to protect sensitive personal information (SPI) such as encryption, access controls etc. After this, customer contracts were reviewed for appropriate protection clauses and service providers were made to sign `reasonable security practices\\' clauses in their contractual obligations as specified in EU GDPR. At first glance, it seemed that XYZ had taken adequate steps to protect SPI dealt by its service providers and ensure that it complies with the regulatory requirements. However, on careful scrutiny, there were some lacunae in the program. For instance, as per EU GDPR, personal data must be pseudonymized or encrypted prior to transfer from one entity to another. In this case, though encryption was mentioned in the policy documents but there were no specific measures given for ensuring proper encryption of data before any transfer. Similarly, `reasonable security practices\\' clause was included in customer contracts but there was no mention of any tools like firewalls or other means of protecting sensitive information which could have further strengthened the privacy protection efforts made by the company. Thus, it is clear that XYZ did made some efforts to comply with the EU GDPR but in order to ensure full compliance, more specific measures should have been taken and all contractual obligations must be such that they clearly define the security and privacy controls that need to be put in place between customer/client and service provider. This would further give customers greater assurance of privacy protection from XYZ\\'s services. Going forward, XYZ can consider investing in more advanced technologies like biometrics authentication etc for maximum security of data. Furthermore, the company should also ensure periodic reviews of its policy documents and contracts so as to ensure better protection of sensitive personal information. Overall, though XYZ took some reasonable steps to protect SPI of its customers, it should have done more by introducing advanced security measures and including stringent contractual obligations for service providers. This would have enabled the company to achieve full compliance with EU GDPR and ensure greater security of customer\\'s personal data.

QUESTION 8

Which of the following statement is incorrect?

A. Privacy policy may be derived from outcomes of privacy impact assessment

B. Misuse of personal information available in public domain may be construed as a privacy violation

C. A privacy policy once framed cannot be changed before the specified review period

D. None of the Above

Correct Answer: C

QUESTION 9

What is a Data Subject? (Choose all that apply.)

A. An individual who provides his/her data/information for availing any service

B. An individual who processes the data/information of individuals for providing necessary services

C. An individual whose data/information is processed

D. A company providing PI of its employees for processing

E. An individual who collects data from illegitimate sources

Correct Answer: AC

QUESTION 10

Classify the following scenario as major or minor non-conformity.

"The organization has a very mature information security policy. Lately, the organization has realized the need to focus on protection of PI. A formal PI identification exercise was done for this purpose and a mapping of PI and security controls was done. The organization has also put in place data masking technology in certain functions where the SPI was accessed by employees of a third party. However, the organization is yet to include PI specifically in its risk assessment exercise, incident management, testing, data classification and security architecture programs."

A. Major

B. Minor

C. Both Major and Minor

D. None of the above

Correct Answer: C

QUESTION 11

With respect to privacy monitoring and incident management process, which of the following should be a part of a standard incident handling process?

I) Incident identification and notification II) Investigation and remediation III) Root cause analysis IV) User awareness training on how to report incidents

A. I and II

B. III and IV

C. I, II and III

D. All of the Above

Correct Answer: D

QUESTION 12

Which among the following would not be characteristic of a good privacy notice?

A. Easy to understand

B. Clear and concise

C. Comprehensive ?explaining all the possible scenarios and processing details making the notice lengthy

D. Multi-lingual

Correct Answer: C

QUESTION 13

The concept of data adequacy is based on the principle of _____.

A. Adequate compliance

B. Dissimilarity of legislations

C. Essential equivalence

D. Essential assessment

Correct Answer: C

QUESTION 14

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 15

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