PassQueen
a.k.a dumpsqueen.com

DSCI Certified Privacy Lead Assessor

DSCI DCPLA

Version Demo

Total Demo Questions: 17

Total Premium Questions: 173

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1 - (SIMULATION)

FILL BLANK

VPI

As a starting point, the consultants undertook a visibility exercise to understand the type of personal information (PI) being dealt with within the organization and also by third parties and the scope was to cover all the client relationships (IT services and BPM both) and functions. They met with the client relationship and business function owners to collect this data. The consultants did a mapping exercise to identify PI and associated attributes including whether company directly collects the PI, how it is accessed, transmitted, stored and what are the applicable regulatory and contractual requirements. Given the enormous scale of the exercise (enterprise wide), the consultant classified the PI as financial information, health related information, personally identifiable information, etc. and collected the rest of the attributes against this classification. When understanding the underlying technology environment, the consultants restricted themselves only to the technology environment that was under company's ownership and premises and did not continue the exercise for client side environment. This was done because relationship owners seemed reluctant to share such client specific details. Only in 2 relationships, were the relationship heads proactive to introduce the consultants to the clients and get the requisite information. The analysis of the environment in these 2 relationships revealed that even though lots of restrictions were imposed at the company side, the same restrictions were not available at the client side.

Many business functions were also availing services from third party service providers. Though these functions were aware of the type of PI dealt by third parties, they were not aware of the technology environment at the third parties. In one odd case, personal information of a company employee was accidentally leaked by the employee of the third party through the social networking site. The consultants relied on whatever information was provided by the functions w.r.t. third parties. After finishing the data collection, the consultant used the information to create information flow maps highlighting the flow of information across systems deployed at the company premises. This work helped them have a high level view of PI dealt by the company. The data collection exercise has been conducted only once by the consultants. The visibility exercise empowered the management to have a company-wide view of PI and how it flows across the organization. This information was coupled with the security controls / practices deployed at the relationship or function level to derive the risk posture of the PI.

(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 FinanceandAccounting 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.

Was the visibility exercise adequately carried out? What gaps did you notice? (250 to 500 words)

ANSWER: Check the explanation for the answer

Explanation:

Conclusion: the visibility exercise was a useful starting point, but it was not adequate for an enterprise-wide privacy programme or for demonstrating GDPR-ready accountability. It produced a high-level view of PI categories and some internal flows, but it did not establish a complete, accurate and maintainable record of processing.

The positive aspects were that the consultants attempted enterprise coverage across client relationships and business functions; identified PI and attributes relating to collection, access, transmission and storage; considered regulatory/contractual requirements; and linked the inventory to existing controls to derive an initial risk posture.

However, significant gaps remain:

Incomplete scope and data-flow mapping: Mapping was restricted to systems owned and hosted on company premises. Client environments, third-party environments, and therefore end-to-end flows, were largely excluded. This is especially material because the two client assessments showed that client-side controls were weaker. Reluctance from relationship owners is not a valid reason to omit relevant processing; it should have been escalated and addressed through client engagement, contractual information rights, and clearly documented shared responsibilities.
Third-party risk was not assessed: Functions merely stated what PI providers handled. XYZ did not validate providers' environments, controls, locations, subcontractors, or breach-management capability. The reported social-media disclosure demonstrates that reliance on unverified statements was inadequate. A supplier inventory, privacy/security due diligence, risk assessment, contractual processor clauses, audit rights and ongoing monitoring were needed.
Inventory was too high-level: Broad labels such as financial, health and PII are useful classifications but do not replace a processing inventory. For each processing activity, XYZ should record the actual data elements, data subjects, business purpose, controller/processor role, recipients, locations/transfers, systems, retention/deletion period, access roles, and applicable legal and contractual obligations. The review should cover the entire lifecycle, including use, disclosure, archival and disposal, not only collection, access, transmission and storage.
No sustainable governance: The collection was conducted once. A defined owner, validation/approval process, periodic review and change-triggered update process are necessary, particularly as client engagements, cloud services, mobility solutions and vendors change.
Privacy risk assessment needs broadening: Security controls alone do not determine privacy risk. The assessment should also evaluate purpose limitation, data minimisation, transparency, individual-rights handling, retention, international transfers, breach response and accountability obligations.

Therefore, the exercise should be expanded into a continuously maintained, validated record of processing and end-to-end data-flow map covering XYZ, clients, cloud/hosting arrangements and all third parties.

QUESTION NO: 2

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

ANSWER: A C

Explanation:

A data subject is the identified or identifiable natural person to whom personal data relates. Therefore, an individual whose data/information is processed is a data subject whenever processing is performed on information relating to that person. This captures the central privacy role: the person is the subject of the information and the person whose privacy interests and data-protection rights are implicated by its collection, use, storage, disclosure, or other handling.

An individual who provides his/her data/information for availing any service is also a data subject where that information relates to the individual. In an ordinary service interaction, a person may supply contact, identity, payment, account, or usage information, and the service provider processes that information to deliver or administer the service. The individual remains the data subject regardless of whether the information was supplied directly by that person or obtained through another permitted source. This understanding aligns with the definition of “data subject” in Article 4 of the GDPR and with India’s analogous concept of a Data Principal under the Digital Personal Data Protection Act, 2023. See GDPR Article 4 definitions and the Digital Personal Data Protection Act, 2023.

QUESTION NO: 3

Section 43A of the Information Technology (Amendment) Act, 2008 holds_____ accountable for having reasonable security practices and procedures in place to protection sensitive personal data.

A. Government

B. Body corporates

C. Government and body corporates alike

D. None of the above

ANSWER: B

Explanation:

“Body corporates” is correct because Section 43A of India’s Information Technology Act, 2000, as amended in 2008, specifically establishes liability for a body corporate that possesses, deals with, or handles sensitive personal data or information in a computer resource. Where that body corporate is negligent in implementing and maintaining reasonable security practices and procedures, and this negligence causes wrongful loss or wrongful gain to a person, it may be liable to pay compensation to the affected person.

The provision is therefore directed at organisations operating as body corporates, rather than creating the same Section 43A obligation for government entities. For operational detail, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 describe reasonable security practices and procedures and specify requirements relevant to sensitive personal data or information. A privacy lead assessor should evaluate whether the relevant body corporate has documented, implemented, and maintained appropriate safeguards proportionate to the data and processing involved. See the Information Technology Act, 2000 on the MeitY website and the 2011 SPDI Rules.

QUESTION NO: 4

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

ANSWER: C

Explanation:

Comprehensive – explaining all the possible scenarios and processing details making the notice lengthy is not a characteristic of a good privacy notice because comprehensiveness must be balanced with usability and intelligibility. A notice should provide individuals with the material information they need to understand how their personal data is handled, including purposes, relevant data categories, recipients, retention, and rights, but it should do so in a structured and accessible way. Attempting to document every conceivable scenario and operational detail in a single notice can obscure the

information that matters most to an individual and makes meaningful reading less likely. Good privacy communication uses clear, concise language and can apply a layered approach: a short, prominent summary presents key points, while additional detail is made readily available through links or expandable sections. This approach supports transparency without overwhelming the reader. The GDPR expressly requires information to be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. See GDPR Article 12 and the UK ICO's guidance on privacy notices.

QUESTION NO: 5

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

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

C. None of the Above

ANSWER: B

Explanation:

"A privacy policy once framed cannot be changed before the specified review period" is the incorrect statement. A review period establishes a planned governance cadence for reassessing the policy, but it does not prevent an organisation from updating its privacy policy sooner. Effective privacy management requires the policy to remain accurate, transparent, and aligned with actual processing practices. Accordingly, an organisation should amend the policy whenever a material trigger arises, such as introducing a new purpose of processing, changing the categories of personal data collected, engaging a new processor, altering retention practices, responding to a significant privacy incident, or accommodating a change in applicable law or regulatory guidance.

Privacy notices and policies are living governance documents rather than static documents that can only be changed on a calendar date. Under India's Digital Personal Data Protection Act, 2023, a Data Fiduciary must provide notice that enables an individual to understand the personal data and purpose of processing; where those details change, maintaining an outdated policy would undermine meaningful transparency. A scheduled review is therefore a minimum control, complemented by event-driven updates, appropriate approval, version control, and communication of material changes. See the Digital Personal Data Protection Act, 2023 and DSCI privacy resources.

QUESTION NO: 6

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

" The organization defined information access and usage policy and rolled it out across the organization No formal exercise, however, was conducted to prepare the policy During implementation, certain discrepancies came out and these were addressed through appropriate policy revisions though this created a lot of hue and cry in the organization and the policy was criticized for adversely affecting productivity But with appropriate revisions and passage of time, the policy has been accepted In a recently conducted external audit one incident has come to light wherein the usage and access policy has been violated by an employee twice As per the auditor this incident should have been identified by the organization In its explanation to the auditor the management informed that appropriate access and usage monitoring mechanisms have been put in place but admitted that there may have been some lapses " .

A. Major

B. Minor

C. Both Major & Minor

D. None of the above

ANSWER: B

Explanation:

Minor is the appropriate classification because the organization has established and deployed an information access and usage policy, revised it in response to implementation findings, and put monitoring mechanisms in place. These facts demonstrate that the underlying control framework exists and is operating, rather than being absent or fundamentally ineffective. The audit finding concerns a lapse in the operation or effectiveness of monitoring: an employee violated the policy twice and the organization did not identify the incident as expected. This should be recorded, investigated, and addressed through corrective action, including determining why the monitoring failed to detect the repeated violation and confirming that detection and escalation processes work consistently going forward.

A minor non-conformity is generally an isolated or limited failure to fully meet a management-system requirement where the overall system remains implemented and capable of achieving its intended outcome. Here, the evidence supports such a limited implementation weakness rather than a breakdown of the access-control policy and monitoring program as a whole. Effective access control also requires review and monitoring of access and associated events, consistent with the control objectives described in ISO/IEC 27001. The finding should therefore lead to proportionate corrective action under the organization's information-security governance processes, as reflected in the Data Security Council of India privacy and security assurance context.

QUESTION NO: 7

Which of the following measures can an organization implement to establish regulatory compliance intelligence? (Choose all that apply.)

A. Establish a process that keeps a track of applicable legal and regulatory changes

B. Identify the liabilities imposed by the regulations with respect to specific data elements

C. Ensure that a mechanism exists for quick and effective provisioning, de-provisioning and authorization of access to information or systems which are exposed to data

D. Ensure that knowledge with respect to legal and regulatory compliances is managed effectively

ANSWER: A B D

Explanation:

Regulatory compliance intelligence is an ongoing organizational capability for identifying, interpreting, organizing, and operationalizing privacy-related legal obligations. "Establish a process that keeps a track of applicable legal and regulatory changes" is essential because privacy requirements, regulator guidance, and sector-specific obligations evolve continually. An organization needs a defined monitoring process so that relevant changes are identified promptly and assessed for their operational impact.

"Identify the liabilities imposed by the regulations with respect to specific data elements" is also central to this capability. Connecting obligations, restrictions, and potential liabilities to particular categories of personal data enables an organization to understand which processing activities require changes, controls, or documented accountability measures.

"Ensure that knowledge with respect to legal and regulatory compliances is managed effectively" supports sustained compliance by making legal interpretations, obligations, guidance, decisions, and updates available to the responsible business, privacy, and compliance stakeholders. Effective knowledge management reduces dependence on informal or isolated expertise and helps ensure consistent implementation across the organization. These measures align with the DSCI focus on building organizational privacy capabilities and with accountability-based privacy governance principles. See the Data Security Council of India and the OECD Privacy Guidelines.

QUESTION NO: 8

Which of the following should be examined by an assessor while evaluating an organization's process for handling requests for access and correction of personal information? (Choose all that apply.)

A. Identity verification of the requester

B. Process to locate relevant personal information

C. Documented response and closure records

D. Automatic rejection of requests involving archived records

E. Assessment of required updates to relevant recipients or systems

ANSWER: A B C E

Explanation:

An effective access and correction process should verify the requester's identity before disclosing or changing personal information. It should also define a method to locate relevant information across the organization's systems and processing relationships. Documented response timelines, approvals, communications, and closure records provide evidence that requests are handled consistently and can be monitored for compliance.

Where information is corrected, the organization should also assess whether relevant recipients, downstream systems, or service providers need to be updated, subject to applicable law and the nature of the processing. A general statement that requests will be considered without a defined workflow is not sufficient evidence of an operational process. These measures support the access and rectification rights in GDPR Articles 15 and 16.

QUESTION NO: 9

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

ANSWER: C

Explanation:

Data Minimization was not expressly prescribed as one of the eight privacy principles in the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, adopted in 1980. The original Guidelines set out the Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability principles. Although data minimization is now a familiar concept in modern privacy laws and frameworks, it was not named as a standalone OECD principle in the 1980 Guidelines.

The closest original concept is the Collection Limitation Principle, which provides that personal-data collection should be limited and obtained by lawful and fair means, generally with the data subject's knowledge or consent. This limitation on collection supports a minimization-oriented outcome, but it is materially different from prescribing "data minimization" as an independent principle. The OECD's later privacy framework continues to identify the original core principles, including openness, security safeguards, and purpose specification. See the OECD Privacy Guidelines and the OECD's Privacy Guidelines overview.

QUESTION NO: 10

With respect to privacy governance, which of the following statements are correct? (Tick all that apply)

A. Privacy governance defines the specifications for privacy operations performed on data processed through computer resource only

B. Privacy governance provides privacy strategy and direction, and takes decisions on key privacy issues

C. Privacy governance addresses day-to-day privacy incidents with processes established by privacy policies and procedures

D. Privacy governance ensures that privacy issues are not left unaddressed in the organization

ANSWER: B D

Explanation:

Privacy governance provides the organizational leadership, accountability structure, decision rights, and oversight needed to manage privacy as an enterprise responsibility. Therefore, *Privacy governance provides privacy strategy and direction, and takes decisions on key privacy issues* is correct: governance establishes the privacy vision, approves priorities, allocates authority, and makes or escalates material decisions such as risk acceptance, policy direction, and responses to significant privacy matters. *Privacy governance ensures that privacy issues are not left unaddressed in the organization* is also correct because a governance framework assigns clear ownership, establishes reporting and escalation routes, and monitors whether privacy obligations, risks, and commitments receive appropriate attention. This supports demonstrable accountability rather than leaving privacy solely to informal or isolated operational activity. The accountability principle in the GDPR requires the controller to be responsible for, and able to demonstrate compliance with, data-protection principles; effective governance is central to meeting that expectation. NIST likewise describes privacy governance as the organizational structures and processes used to manage privacy risk and accountability. See GDPR, Article 5(2) and the NIST Privacy Framework.

QUESTION NO: 11

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

ANSWER: D

Explanation:

"Processing is a blanket term used for the wide range of operations performed on personal data" is correct because processing is deliberately defined broadly in privacy law. It encompasses the full data life cycle and can include collecting, recording, organising, structuring, storing, adapting, retrieving, using, disclosing, sharing, restricting, erasing, and destroying personal data. The particular operation may be performed manually or by automated means; it is still processing when it is carried out in relation to personal data.

This broad interpretation is important to a privacy lead assessor because privacy obligations and controls must be assessed across every activity involving personal data, rather than being limited to one operational stage such as collection, storage, or deletion. The Digital Personal Data Protection Act, 2023 defines processing as an automated operation or set of operations performed on digital personal data, including collection, recording, storage, use, sharing, disclosure, and erasure. Likewise, the GDPR's definition illustrates the breadth of the term through a non-exhaustive list of activities. See the Digital Personal Data Protection Act, 2023 and GDPR, Article 4.

QUESTION NO: 12

As a privacy lead assessor assessing the company for DSCI's privacy certification, you are assessing the adequacy of resources and skills in the organization, to address privacy related responsibilities.

Which DSCI Privacy Framework (DPF©) practice area is relevant?

A. Visibility over Personal Information (VPI)

B. Privacy Organization and Relationship (POR)

C. Privacy Awareness and Training (PAT)

D. Information Usage and Access (IUA)

ANSWER: B

Explanation:

Privacy Organization and Relationship (POR) is the relevant DSCI Privacy Framework practice area because assessing whether privacy responsibilities are supported by adequate people, skills, authority, and resources is fundamentally an organizational-governance activity. A privacy programme cannot operate effectively merely through documented policies; the organization must establish an appropriate privacy structure, assign accountability, define relevant roles and reporting relationships, and ensure that personnel responsible for privacy have the competence and capacity to perform their duties.

During an assessment, this includes examining whether the privacy function has sufficient staffing and access to expertise, whether responsibilities are clearly allocated across business and support functions, and whether privacy personnel can coordinate with key internal and external stakeholders. The assessment should also consider whether the organization's governance arrangements allow privacy requirements and decisions to be escalated, monitored, and implemented consistently. These elements directly demonstrate that privacy responsibilities are embedded in the organization rather than being informal or unsupported.

DSCI's privacy programme and certification resources position organizational accountability and implementation capability as key elements of a mature privacy framework. See DSCI Privacy and DSCI Certification.

QUESTION NO: 13

What are the criteria for deciding the role of Data Fiduciary? Tick all that apply.

A. Data Fiduciary is the one who decides the means of personal data processing

B. Data Fiduciary is the one who acts on behalf of data processor

C. Data Fiduciary is the one who stores the personal data

D. Data Fiduciary is the one who decides the purposes of personal data processing

ANSWER: A D

Explanation:

Under section 2(i) of India's Digital Personal Data Protection Act, 2023, a Data Fiduciary is a person who, alone or together with other persons, determines *the purpose and means* of processing personal data. Therefore, deciding the purposes of personal-data processing and deciding the means of personal-data processing are both essential criteria for identifying this role. "Purpose" concerns the reason or intended outcome for which personal data is processed, such as providing a service, conducting recruitment, or managing customer relationships. "Means" concerns the material decisions about how that processing is carried out, including the systems, methods, categories of data, retention approach, and processing arrangements used to achieve the purpose. The Act's definition also recognizes that these decisions may be made jointly, so more than one organization can be a Data Fiduciary where they collectively determine those elements. This distinction is central to accountability under the Act because the entity determining these processing decisions is responsible for ensuring that personal data is processed in accordance with the applicable legal obligations. The statutory definition can be consulted in the Digital Personal Data Protection Act, 2023 on India Code and on the Ministry of Electronics and Information Technology website.

QUESTION NO: 14 - (SIMULATION)

FILL BLANK

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 FinanceandAccounting 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)

ANSWER: Check the explanation for the answer

Explanation:

Answer: I do not agree with using one detailed privacy policy as the only policy for every relationship and function. XYZ may establish a short, enterprise-wide privacy policy that states common principles, governance, accountability, baseline safeguards, incident handling, and compliance obligations. However, it must be supported by business-, client-, jurisdiction-, and processing-specific procedures, privacy notices, and contractual controls.

XYZ performs very different roles: it may act as a processor/service provider for clients, a controller for employee or direct customer information, and possibly a joint controller in some platform or cloud arrangements. The personal-information categories, purposes, legal bases, retention periods, recipients, cross-border transfers, and data-subject rights will differ materially between a payroll process, credit-card processing, healthcare BPM, a cloud platform, and government projects. A single lengthy document cannot clearly or accurately prescribe all these requirements. It has already failed the usability test: relationship and functional heads cannot relate its requirements to their activities or identify their actions.

Further, a policy is not the same as a privacy notice. Publishing an internal policy on the intranet and circulating it to business heads does not satisfy transparency obligations toward individuals. Assuming XYZ directly collects personal information from a client's end customers, XYZ must determine its role under the applicable law and contract. If it is an independent or joint controller, it should provide a clear, accessible, layered external privacy notice to those individuals,

including required GDPR information where GDPR applies. If XYZ collects information solely as the client's processor, the client/controller normally provides the notice, while XYZ's processing must be governed by a data-processing agreement and documented instructions. The contractual allocation of notification duties should be explicit.

I recommend the following structure:

Enterprise policy: concise mandatory privacy principles and minimum controls applicable to all staff.
Standards and procedures: role-based procedures for collection, access, sharing, retention/deletion, breach escalation, data-subject requests, DPIAs, vendor management, and international transfers.
Processing-specific documents: client/account playbooks and data maps that state the data, purpose, role, applicable laws, approved actions, and responsible owner.
Audience-specific notices and training: separate employee, website/app, cloud-product, and other external notices; concise role-based training rather than a single one-day workshop for all heads.

Thus, consistency should be achieved through a common privacy framework, not through one complex policy that obscures the operational and legal differences among XYZ's services.

QUESTION NO: 15

Which of the following are appropriate measures for demonstrating the effectiveness of privacy monitoring? (Choose all that apply.)

A. Review access logs for unusual access to personal information

B. Test retention and deletion controls against approved schedules

C. Track corrective actions arising from privacy incidents and findings

D. Retain monitoring reports without assigning an owner for review

E. Report material privacy metrics and trends to management

ANSWER: A B C E

Explanation:

Privacy monitoring should provide evidence that controls are operating as intended and that identified weaknesses are addressed. Periodic review of access logs can identify unauthorized, unusual, or excessive access to personal information. Testing whether retention and deletion controls operate according to approved schedules verifies that documented requirements are implemented in practice.

Tracking privacy incidents, complaints, findings, and corrective actions helps management identify recurring issues and confirm closure. Reporting meaningful metrics to management supports accountability and enables informed decisions on resources and risk treatment. Merely collecting monitoring data without review or follow-up does not demonstrate effectiveness. These practices align with the accountability and security expectations in GDPR Articles 5, 24 and 32 and the NIST Privacy Framework.

QUESTION NO: 16

CORRECT TEXT

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.

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

500 words)

A. Seetheanswerinexplanationbelow.

B. The company lacked auditable change-management and remediation evidence to demonstrate that the vulnerability was fixed, while weak regulatory and contractual requirements management prevented clear accountability.

ANSWER: B

Explanation:

The company failed to defend itself because it lacked accountable, auditable evidence that the assigned vulnerability remediation had been implemented, when it had been implemented, and whether the change remained effective in the production environment. A defensible privacy and security control environment requires formal change management: an approved remediation ticket, risk and impact assessment, identified owner, implementation record, testing or validation

results, production deployment evidence, timestamps, and retained logs. These records establish traceability from the third-party assessment finding through closure and enable the processor or service provider to demonstrate performance of its contractual obligations.

The case also supports the need for a structured regulatory and contractual compliance process. The organization should maintain a current obligations register, translate relevant legal and client contractual requirements into specific control requirements, assign ownership, and collect evidence of ongoing operation. For sensitive health information, the absence of reliable evidence is particularly material because breach response and accountability depend on accurate facts about the vulnerability, remediation, and dates. The GDPR accountability principle similarly requires an organization to be able to demonstrate compliance, while its security provision requires appropriate technical and organisational measures. See Regulation (EU) 2016/679, Articles 5 and 32. A documented audit trail, supported by configuration baselines and verification records, would have enabled the company to substantiate its position to the client.

QUESTION NO: 17

Which of the following practices support implementation of the Collection Limitation principle? (Choose all that apply.)

A. Document the purpose for collecting each data element

B. Remove data fields that are not necessary for the stated purpose

C. Make all fields mandatory to improve completeness of records

D. Periodically review collection forms and digital interfaces

E. Collect additional data for unspecified future use

ANSWER: A B D

Explanation:

Collection Limitation requires an organization to collect personal information only where it is relevant and necessary for a defined purpose. Documenting the purpose before collecting a data element helps establish the business justification for the collection. Reviewing forms and digital interfaces to remove fields that are not necessary directly reduces excessive collection.

Applying controls to prevent optional fields from being treated as mandatory supports meaningful choice and data minimisation. Periodic review of collection practices is also important because business processes and data needs can change over time. Retaining every field merely because it may be useful in the future is inconsistent with necessity and minimisation. These practices align with data minimisation under GDPR Article 5 and with the collection-limitation principle in the OECD Privacy Guidelines.