DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Moving to Cloud-based Solutions

Key considerations for public sector enterprises

Supported by

THE BEST RUN SAP®

September 2021

Copyright & Disclaimer

This report has been developed by Data Security Council of India (DSCI).

Data Security Council of India

The information contained herein has been obtained or derived from sources believed by DSCI to be reliable. However, DSCI disclaims all warranties as to the accuracy, completeness or adequacy of such information. We shall bear no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof.

The material in this publication is copyrighted. You may not, however, distribute, modify, transmit, reuse or use the contents of the report for public or commercial purposes, including the text, images, presentations, etc. without DSCI's prior consent.

Introduction

The rate of adoption of cloud services in the public sector has been on the rise. NASSCOM predicts that cloud spending in India is estimated to grow at 30% p.a. to reach USD7.1-7.2 Bn by 2022 [1]. Public sector enterprises have been looking at cloud as one of the critical technology choices in their journey towards digitization. However, it is essential for public sector enterprises to be prudent in their selection of cloud service partners to minimise recurrent issues. These issues may stem from complexities associated with service integration, data residency, contractual safeguards and user privacy. It is vital to appreciate these apprehensions and examine them holistically during the pre-procurement engagement with the service provider.

Cloud service providers have made considerable efforts to demonstrate that they have addressed the concerns of the market with respect to data security and privacy of the data uploaded to their services. Some providers will also have robust and independently verified security credentials that are designed to meet the specific needs of their target markets. This has helped slowly erode some of the resistance towards cloud adoption by public sector enterprises. However, public sector enterprises must also take cognizance of the changes required to make the most of the capabilities offered by the service provider [2].

This paper examines these concerns and provides a short guide for decision makers who are accountable for information risk and other senior personnel who need to make proportionate and risk-aware choices when considering the purchase of cloud services for enterprise use.

The key considerations to examine from the perspective of cloud service adoption can be categorized into the following:

A. **Privacy considerations:** Sensitive data exposure and utilization; transparency and accountability measures and individual rights.

B. **Data Residency considerations:** Movement of data across geographies and jurisdictions, and the protection of the data against unintended access and other location-related risks.

C. **Security considerations:** Measures employed to safeguard the data residing on cloud and necessary technical controls.

D. **Contractual considerations:** Provisions associated with applicable law and jurisdiction, security safeguards, sub-contracting, etc.

The aforementioned considerations would assist decision makers in gauging whether the service provider is the right fit for their enterprise. The presence of established best practices and safeguards has become an important market differentiator, as it speaks to the services provider's commitment towards maintaining transparency in operations, whilst providing quality service.

A

Privacy Considerations

These considerations arise from a careful assessment of user expectations of control over their personal data, regulatory expectations surrounding personal data storage and replication in a specific jurisdiction; legal accountability for personal data protection and the nature of personal data being processed using the cloud solution.

Sensitive Personal Data Exposure and Utilization

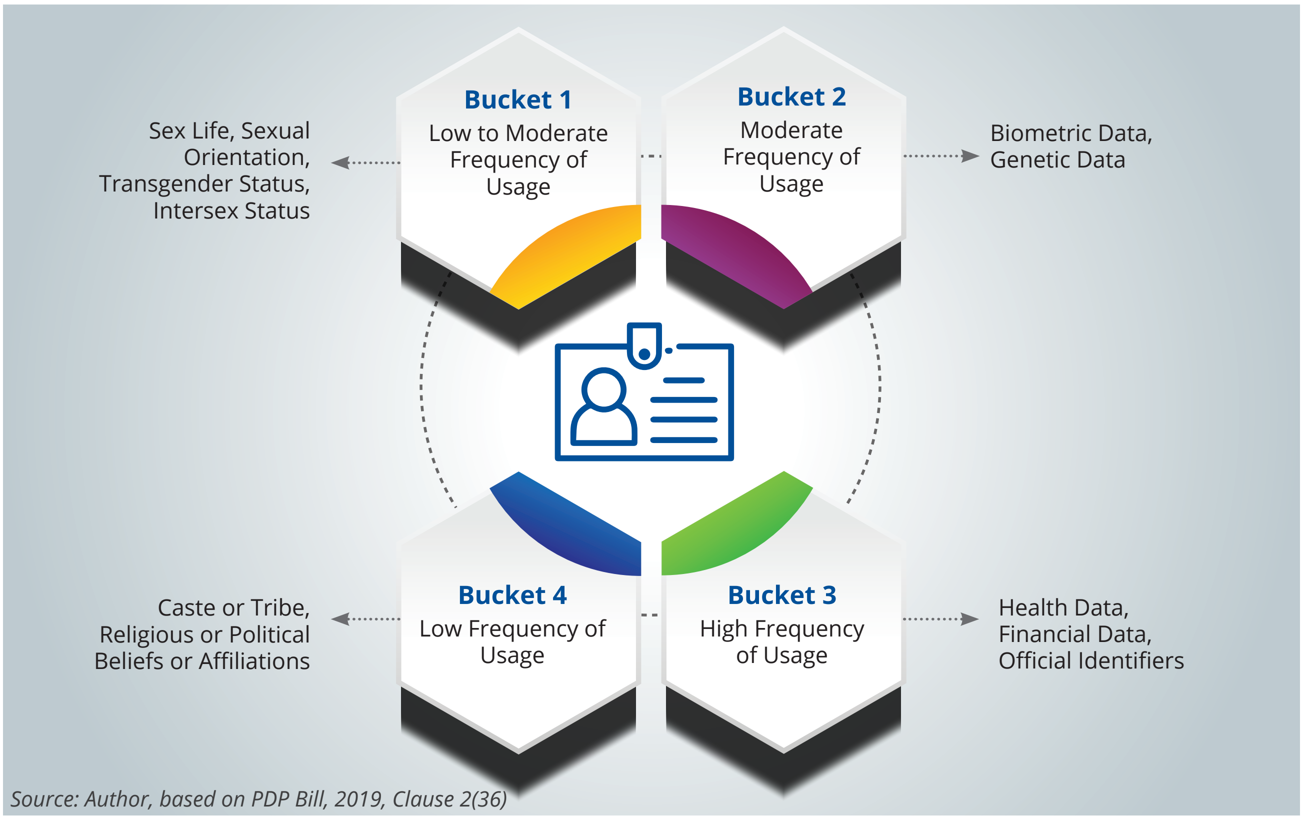
Public sector enterprises decision makers must evaluate the type of personal data being processed as a part of the service offering and note any regulatory or legislative requirements associated with such data. The enterprise must also gauge the competence of the service provider to meet the said regulatory or legislative compliance requirements.

Sensitive Personal Data (SPD) is a subset of Personal Data[3]. The processing of such SPD could create a significant risk to the individual especially in relation to their fundamental rights and freedoms. The classification of SPD is on the basis of country, society and culture specific. In India, what may be categorized as SPD is laid down under Rule 3 of the SPD, or (Information under reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 [4].

The processing of SPD attracts the application of additional safety measures and guarantees that need to be operationalized by the data processing entities, that is, data controllers[5] and data processors[6]. These additional measures consist of maintaining higher standards of user consent (explicit consent) for processing and conducting a data protection impact assessment to gauge the risk of processing such data, on top of other transparency and accountability measures covered in the next subsection.

The Indian privacy legislative landscape is going through a transformative phase with the Personal Data Protection Bill, 2019 on the horizon. The bill adopts a rights-based approach to privacy and creates a principal-agent relationship between data principals[7] and data fiduciaries[8]. It places importance on the requirement of free, informed, specific and clear consent. The SPD categorization has also been augmented to include new data types. The following figure showcases the new classification and frequency of utilization of the data types by the industry at large.

Figure 1: SPD Classification under PDP Bill 2019 and Frequency of Usage


Bucket 1
Low to Moderate Frequency of Usage
Sex Life, Sexual Orientation, Transgender Status, Intersex Status
Bucket 2
Moderate Frequency of Usage
Biometric Data, Genetic Data
Bucket 4
Low Frequency of Usage
Caste or Tribe, Religious or Political Beliefs or Affiliations
Bucket 3
High Frequency of Usage
Health Data, Financial Data, Official Identifiers

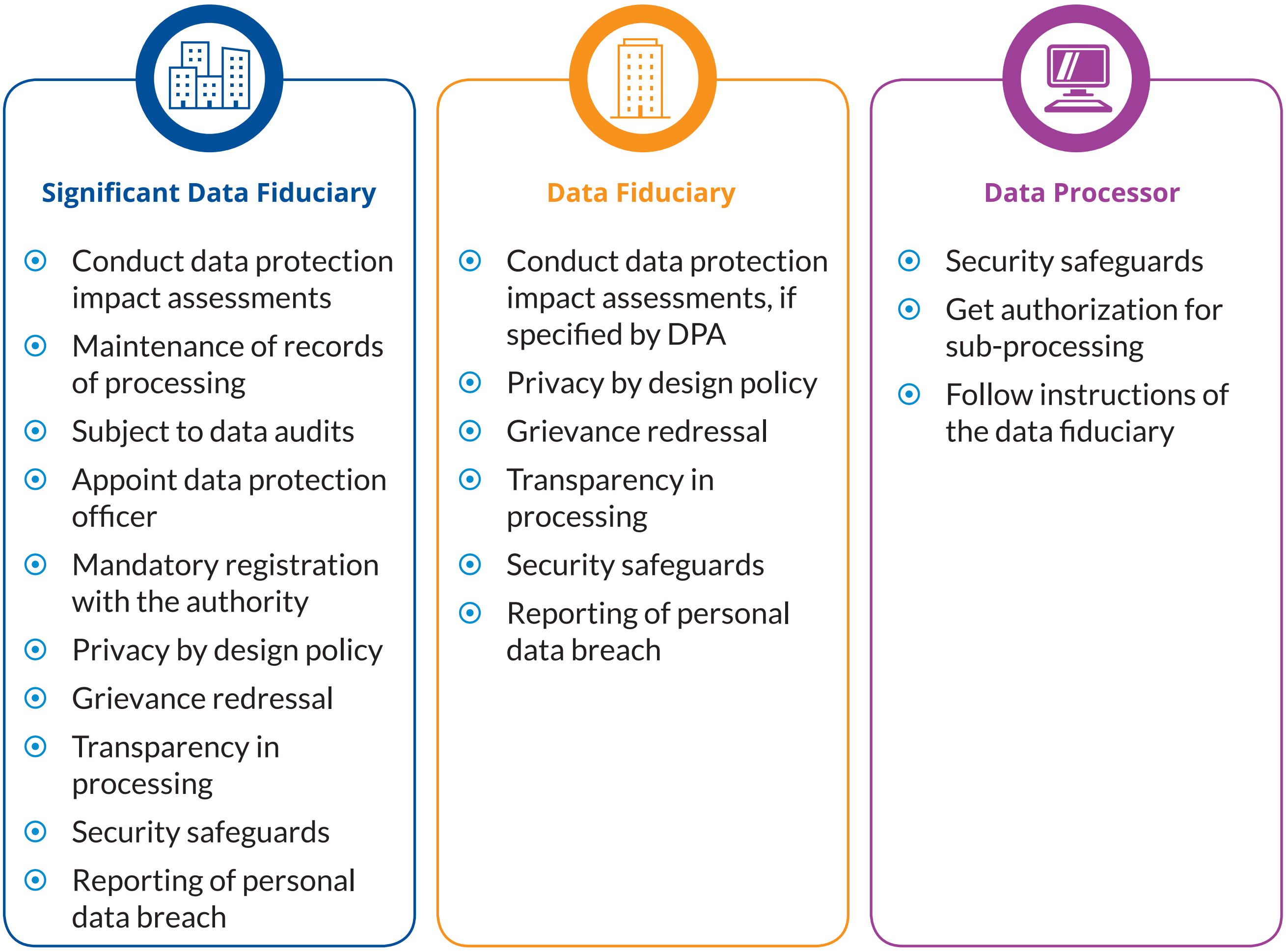
Source: Author, based on PDP Bill, 2019, Clause 2(36)

Transparency and Accountability

> **The enterprise decision makers while evaluating a cloud service offering must evaluate the capability of the service provider to meet compliance requirements and the existence of established practices to assist the enterprise in meeting their share of compliances. These compliance requirements are collectively denoted as transparency and accountability measures.**

Another important point of consideration for an enterprise with respect to personal data processing is ascertaining the accountability chain for the data in question. The exposure to a new environment may lead to changes in ownership levels and measures to be implemented to sustain the processing activity. The Personal Data Protection Bill, 2019, provides a new system of categorization for data processing entities, that is, significant data fiduciaries[9], data fiduciaries and data processors. These processing entities are required to implement differential measures based on their role in the processing chain. With the significant data fiduciaries attracting a majority of the transparency and accountability measures and the data processors attracting the least. The figure below showcases the various measures that need to be taken by each of the entities.

Figure 2: Segregation of Duties under PDP Bill 2019



Significant Data Fiduciary

- Conduct data protection impact assessments
- Maintenance of records of processing
- Subject to data audits
- Appoint data protection officer
- Mandatory registration with the authority
- Privacy by design policy
- Grievance redressal
- Transparency in processing
- Security safeguards
- Reporting of personal data breach

Data Fiduciary

- Conduct data protection impact assessments, if specified by DPA
- Privacy by design policy
- Grievance redressal
- Transparency in processing
- Security safeguards
- Reporting of personal data breach

Data Processor

- Security safeguards
- Get authorization for sub-processing
- Follow instructions of the data fiduciary

Source: Author, based on Clause 26 and Chapter VI – Transparency and Accountability Measures, PDP Bill, 2019.

Salient Transparency and Accountability Measures

The presence of the following measures should be evaluated by the enterprise to gauge the privacy maturity of the cloud service provider.

Data Protection Impact Assessment

I. It's a process by which companies can systematically assess and identify the privacy and data protection impacts of any products they offer and services they provide. It enables them to identify the impact and take the appropriate actions to prevent or, at the very least, minimize the risk of the impacts.

II. DPIA should be used to assess new systems, significant changes to existing systems, operational policies and procedures and intended use of the information. An effective DPIA evaluates the sufficiency of privacy practices and policies with respect to existing legal, regulatory and industry standards, and maintains consistency between policy and operational practices.

Privacy by Design

I. It's a practice through which an organization builds privacy directly into technology, systems and practices at the design phase, thereby ensuring privacy at the outset.

II. Privacy by Design consists of seven foundational principles: (1) Proactive not Reactive; Preventative not Remedial (2) Privacy as the Default Setting (3) Privacy Embedded into Design. (4) Full Functionality—Positive-Sum, not Zero-Sum (5) End-to-End

Security—Full Lifecycle Protection. (6) Visibility and Transparency—Keep it Open and (7) Respect for User Privacy—Keep it User-Centric [10].

III. Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Reporting of Personal Data Breaches

I. Personal Data Breach Reporting refers to the practice of alerting and informing stakeholders including data principals that a personal data breach has occurred. The nature of reporting required depends on the nature of data involved in the breach.

II. A demonstrable ability for detection and reporting of the breach to the enterprise in line with contractual and statutory requirements is an important consideration before on-boarding a new service provider.

Data Principal Rights

The enterprise, while evaluating a cloud service offering, must evaluate the capability of the service provider to enable execution of data principal rights and the existence of established practices to assist the enterprise in meeting the privacy expectations of the individual. These compliance requirements should be viewed from the perspective of cultivating user trust, with due regard to the reputational risk associated with non-compliance.

The primary responsibility for executing data principal rights rests with the data fiduciary (controller) but the data processor should have the competence to assist the data fiduciary in the execution of rights. This ability of the service provider would be of utmost importance with the upcoming personal data protection law in India.

The Personal Data Protection Bill, 2019, lays down different rights for the individual to exercise. These are as follows:

Confirmation and Access

I. The data principal shall have the right to obtain from the data fiduciary a confirmation whether the data fiduciary is processing or has processed personal data of the data principal [11].

II. Provide a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal.

III. The data principal shall have the right to access from one place, the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations [12].

Data Portability

I. Where the processing has been carried out through automated means, the data principal shall have the right to receive the personal data in a structured, commonly used and machine-readable format, capable of being transferred to any other data fiduciary [13].

II. Such personal data would include the personal data provided to the data fiduciary; the data that has been generated in the course of provision of services or use of goods by the data fiduciary; or the data that forms a part of any profile on the data principal, or which the data fiduciary has otherwise obtained [14].

Right To Be Forgotten

I. The data principals have the right to restrict or prevent the continuing disclosure of his/ her personal data by a data fiduciary where such disclosure—(a) has served the purpose for which it was collected or is no longer necessary for the purpose; (b) was made with the consent of the data principal and such consent has since been withdrawn [15].

II. It may be enforced only with an order of the Adjudicating Officer made on an application filed by the data principal [16].

Correction and Erasure

I. The data principal shall where necessary, having regard to the purposes for which personal data is being processed, have the right to—(a) the correction of inaccurate or misleading personal data; (b) the completion of incomplete personal data; (c) the updating of personal data that is out-of-date; and (d) the erasure of personal data no longer necessary for the purpose for which it was processed [17].

II. Where the data fiduciary corrects, completes, updates or erases any personal data, such data fiduciary shall also take necessary steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, updation or erasure, particularly where such action may have an impact on the rights and interests of the data principal or on decisions made regarding them [18].

B

Data Residency Considerations

The enterprise's decision makers must evaluate the applicable regulatory landscape to ascertain the existence of any data residency requirement stemming from any government directive (state/central/sectoral) or a statute before onboarding a cloud-based service provider.

Data residency is the set of issues and practices related to the location of data and metadata. It also relates to the movement of data across geographies and jurisdictions, and the protection of that data against unintended access and other location-related risks [19].

"Data" is not limited to personal data or patient health information (PHI), or generally to data covered by data protection regulations that typically focus on the privacy of individuals. This is why data residency is not the same as privacy, even though they are related [20].The confusion between the two concepts is common and understandable, but the distinction is important:

I. An organization may keep certain data within a single location, even on its own premises, thus avoiding data residency issues, and still violate privacy. For example, a manufacturing company whose administrative personnel has unrestricted access to sensitive information about individual workers, causing concerns for privacy of the workers.

II. An organization may place data that has no privacy implications in a location that causes a data residency issue. For example, this would be the case of a power company that stores corporate financial records of a client in a country where authorities may demand access to the information as a result of a tax dispute.

Even organizations that do not use cloud solutions are often exposed to data residency issues. For example, if an organization:

I. Consolidates multiple data centers from different countries into a single location in a different country from some of the initial locations,

II. Remotely backs up or mirrors data across borders to provide disaster recovery and business continuity,

III. Receives warranty or technical support from personnel located in another country,

IV. Outsources some business processes to another country, for example to lower costs or to access expertise not available at home.

Data residency issues are most often raised in the context of legal and regulatory constraints, as in the above examples. However, the above definition also covers the potential loss or degradation of reliability, service delivery, security, speed, or business continuity.

Personal Data Transfers and Local Storage

It is imperative for the enterprise's decision makers to understand the enterprise's personal data spread and the requirements that emerge from the processing of such data. The solution must be flexible enough to allow for changes to be made to ensure meaningful compliance for the enterprise.

As elaborated in the previous section, residency issues arise for a variety of reasons. A major reason being legal or regulatory constraints around transfer and local storage of personal data. The enterprise must evaluate the applicable regulatory landscape for such regulatory requirements before onboarding a cloud-based service provider.

Presently, SPDI Rules, 2011 that represents the existing framework for personal data protection in India, allows transfer of SPD or information to outside India, provided the transfer is necessary for the performance of the lawful contract between the corporate body or any person on its behalf and the provider of the information or where such person has consented to data transfer. The data import country must adhere to the same level of data protection as prescribed under the SPDI Rules, 2011.

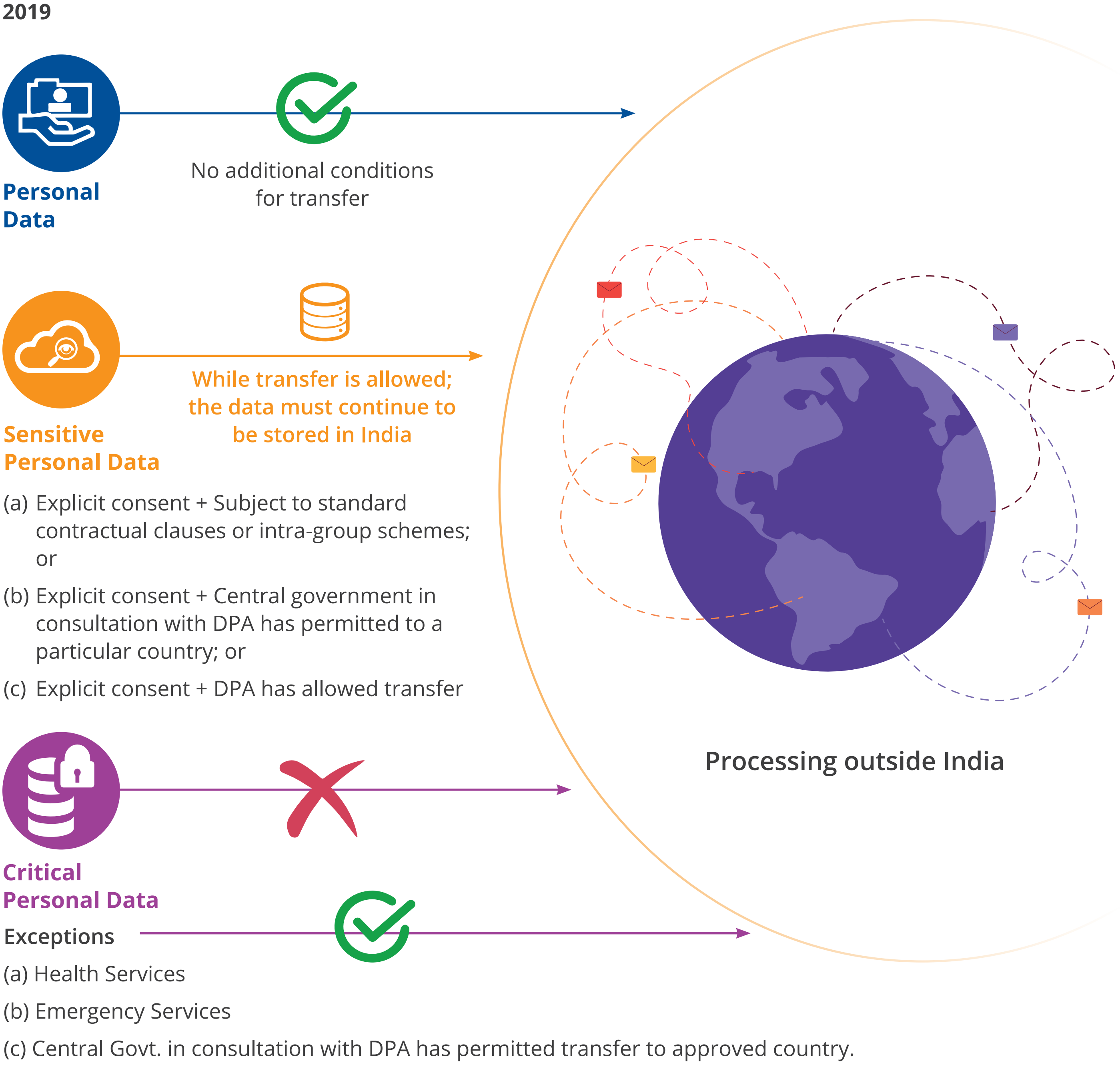
The Personal Data Protection Bill, 2019, lays down differential provisions for transfer and localization of different categories of personal data. There are no restrictions on transfer of personal data outside the Indian territory, but the bill does restrict the transfer of SPD and critical data.

Clause 33 specifies that SPD may be transferred outside of India but must continue to be stored in India. In effect, a local copy of all SPD must remain within India at all times.[21]

SPD is defined broadly in Clause 3(36) of the PDPB and constitutes “personal data, which may, reveal, be related to, or constitute financial data; health data; official identifier; sex life; sexual orientation; biometric data; genetic data; transgender status; intersex status; caste or tribe; religious or political beliefs or affiliation; or any other data categorized as sensitive personal data under section 15”. Section 15 of the PDPB permits the central government to classify further categories of personal data as SPD [22].

Clause 33 further notes that critical personal data may only be processed in India. Coupled with the fact that critical personal data can only be transferred outside of India under limited circumstances (see figure below), this effectively creates a data localization requirement for critical personal data in India. The bill leaves the definition of “critical personal data” to the central government [23].

Figure 3: Restrictions and Conditions for Transfer of Personal Data Outside India under PDP Bill, 2019



Personal Data

No additional conditions for transfer

Sensitive Personal Data

While transfer is allowed; the data must continue to be stored in India

(a) Explicit consent + Subject to standard contractual clauses or intra-group schemes; or

(b) Explicit consent + Central government in consultation with DPA has permitted to a particular country; or

(c) Explicit consent + DPA has allowed transfer

Critical Personal Data

Exceptions

(a) Health Services

(b) Emergency Services

(c) Central Govt. in consultation with DPA has permitted transfer to approved country.

Processing outside India

Clause 34 of the PDPB outlines the circumstances in which sensitive personal data and critical personal data may be transferred outside of India. SPD may only be transferred outside of India for processing purposes when explicit consent is given by the data principal for the transfer, and the transfer is made (1) pursuant to a contract or intra-group scheme approved by the Indian DPA; or (2) where the central government has made an "adequacy" finding with respect to a particular country, entity, class of entity in a country or international organization; or (3) where the DPA has allowed the transfer of any sensitive personal data, or class of such data, necessary for any specific purpose [24].

The public sector enterprise must have complete visibility over the nature of data to be uploaded to the cloud service. It should exercise governance over any disclosure to limit the data spread, and the scope of compliance.

CASE STUDY

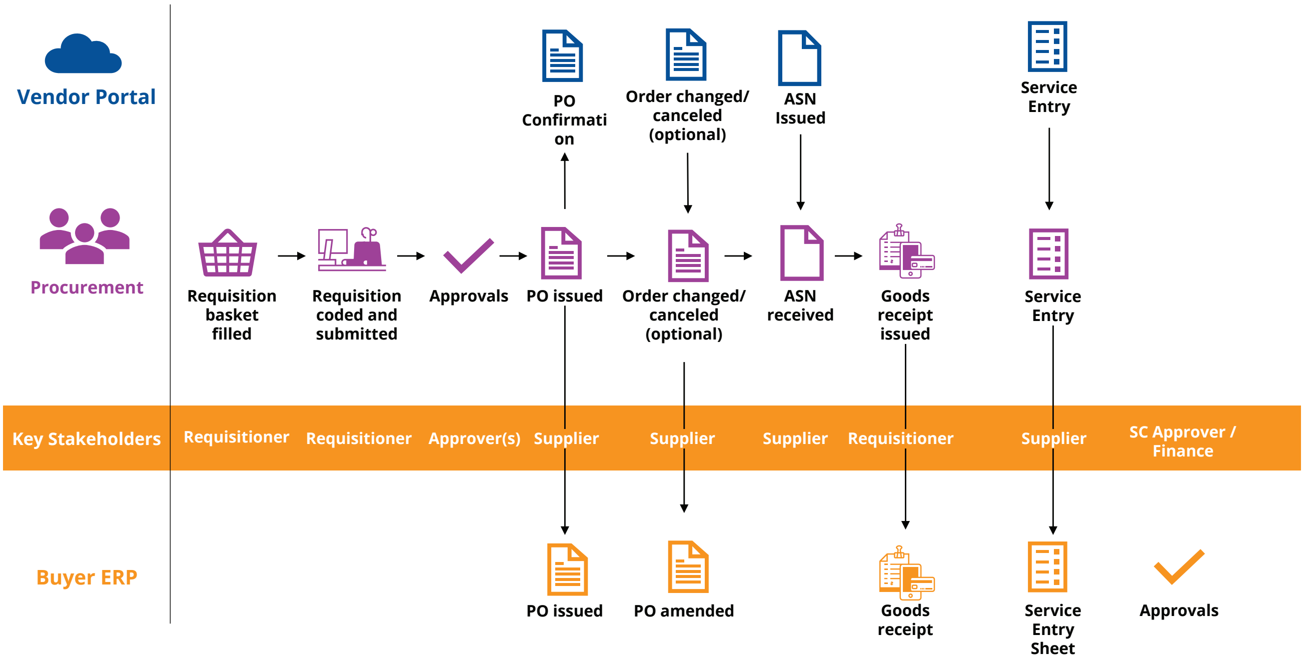
Assessing privacy and residency considerations for SaaS Procurement Solutions

SaaS procurement solutions are one of the most prevalent solutions utilized by public sector enterprises. While considering a procurement solution provider, the security and privacy decision makers of the organization must consider the data collected and utilized during the different operations performed while using the solution, such as **ordering & delivery process, supplier registration & onboarding, supply chain collaboration and invoicing and payment.**

1. Ordering & Delivery process

During this process, the end user raises a request on a pre-approved catalogue with the supplier. The entire delivery mechanism, collaboration with supplier happens over a portal or through a mobile application.

Figure 4: Process Flow & Architecture



Source: Author, based on stakeholder discussions

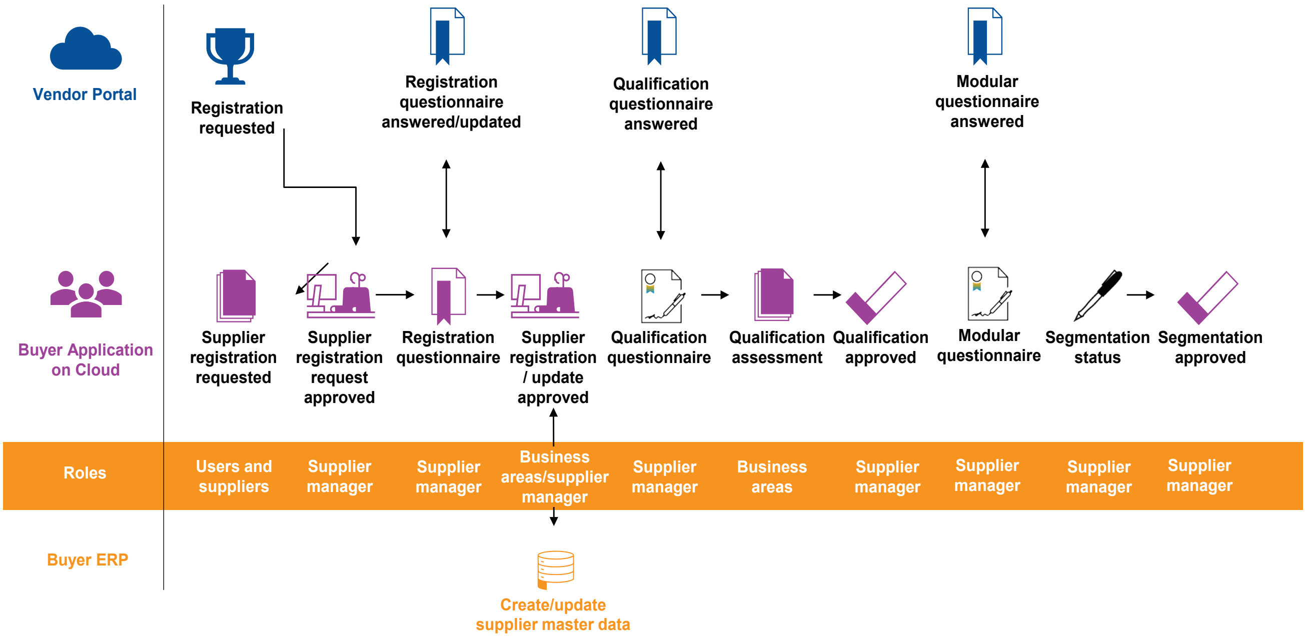
Data collected and used during this process mostly consists of non-personal data such as Commodity Code Item Code, Item Description, Service Unit Price, Service Period, Approval Flow, etc. and Personal data comprising of Employee User – Name, Employee User – Email, Employee User – Phone, Employee User – Address, etc.

Sensitive data is not collected during this operation. Hence, this type of processing activity would not attract the regulatory requirements associated with sensitive data processing in India such as data residency.

2. Supplier Registration and Onboarding

Organizations view supplier registration and onboarding as a way of having a qualified supplier database to procure goods and services from, with agreed terms, and purchasing clauses. A typical process consists of supplier registration, supplier qualification, supplier evaluation, supplier classification and records update, supplier master record creation.

Figure 5: Process Flow and Architecture


Vendor Portal
Registration requested
Registration questionnaire answered/updated
Qualification questionnaire answered
Modular questionnaire answered
Buyer Application on Cloud
Supplier registration requested
Supplier registration request approved
Registration questionnaire
Supplier registration / update approved
Qualification questionnaire
Qualification assessment
Qualification approved
Modular questionnaire
Segmentation status
Segmentation approved
Roles
Users and suppliers
Supplier manager
Supplier manager
Business areas/supplier manager
Supplier manager
Business areas
Supplier manager
Supplier manager
Supplier manager
Supplier manager
Buyer ERP
Create/update supplier master data

Source: Author, based on stakeholder discussions

Data collected and used during this process mostly consists of non-personal data such as Supplier Company – Name, Email, Supplier Company – Phone, Supplier Company – Address, Supplier Company – Profile, Supplier Company Identification, Supplier GST Id, Supplier Tax Id, Supplier PAN, Supplier Company Bank Account Details, etc.

And personal data such as Supplier Contact Person – Name, Supplier Contact Person – Email, Supplier Contact Person – Phone, Supplier Contact Person – Address, etc.

The non-personal data processed as a part of this operation would not attract any privacy related compliance requirements. The personal data would require transparency and accountability safeguards to guarantee protection of such personal data. Sensitive data is not collected during this operation. Hence, this type of processing activity would not attract the regulatory requirements associated with sensitive data processing in India such as data residency.

3. Supply Chain and Delivery Process

Supply Chain Management with external stakeholders is essential for coordinated manufacturing and deliver as per the demand from the market. Organizations incorporate Supply Chain Collaboration, through implementing a planning exercise, sharing the forecast, inventory status with external parties for timely shipment of the required materials.

Typical Supply Chain Collaboration involves following activities: Share Forecast (Forecast Collaboration), Share Inventory (Supplier Managed Inventory), Subcontracting Commitments (Subcon Purchase Orders/ Scheduling Agreements), Inbound Quality Checks (Quality Management/Notifications), Vendor Payments (Self Billing – Evaluated Receipts Settlement).

Figure 6: Process Flow and Architecture

		BUYER	NETWORK	SUPPLIER
Planning	Forecast Collaboration	Share forecast	⟷	Forecast commit
	Supplier Managed Inventory	Share demand, inventory and min/max levels	⟷	Share demand, inventory and min/max levels
	External Manufacturing Visibility		←	Provide Manufacturing and Inventory Status
Procurement	PO Collaboration (all PO types)	Place Order with Delivery Schedule	⟷	Confirm order and provide advanced shipment notification
	Vendor Consignment	Report consumption of consigned stock	⟷	Consignment movement and settlement visibility
	Scheduling Agreement Release	Provide rolling delivery schedule w/different firming levels	⟷	Execute against firmed orders (released)
	Subcontract/ Contract Manufacturing w/ Multi-tier orders	Place order with components Provide notification of components' shipment Provide component inventory & order visibility	⟷	Notify buyer of components' receipt Provide component consumption
	Quality Notifications Quality Inspections Quality Reviews	Communicate & respond to quality notification Request test results, COC, COA Collaborate and share quality documents	⟷ →	Request & respond to quality notification Submit test results, COC, COA Collaborate and share quality documents
Invoice Management	Vendor Invoice Processing	Provide invoice processing status & payment notification	⟷	Provide invoice based on PO/ASN
	Self-Billing/ERS Invoicing	Provide self-bill/ERS invoice based on GR Provide payment notification	→	Invoice Status Visinility
	Return Order Collaboration	Place return order & provide return ship notice	⟷	Provide credit memo

Source: Author, on the basis of stakeholder consultations

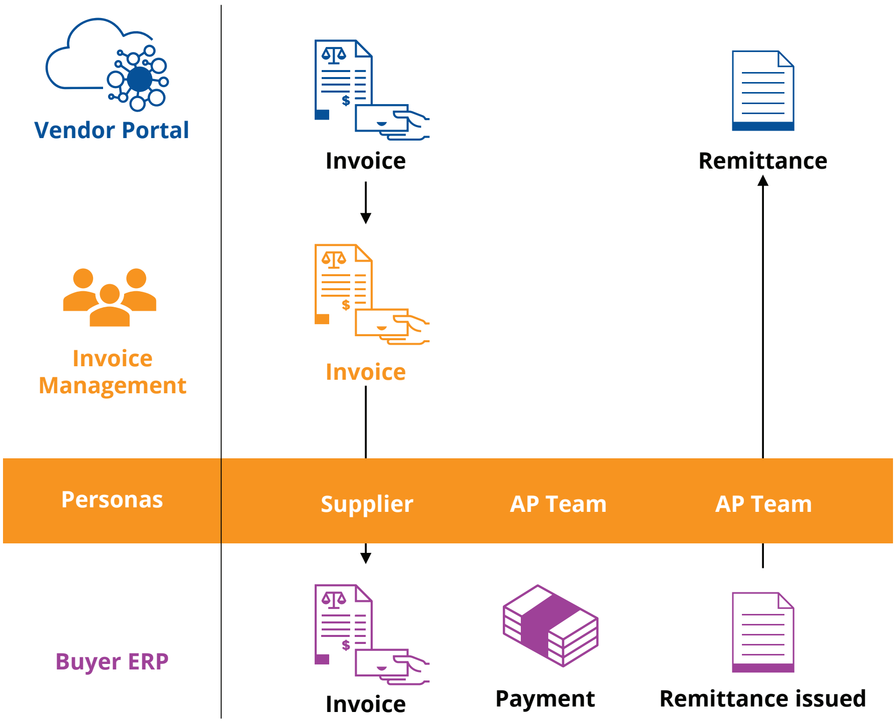
Data collected and used during this process consists of Non-Personal Data such as Purchase Order Confirmation Number, Estimated Shipping Date, Estimated Delivery Date, Original PO Details, Packing Slip number, Shipping Date, Expected Delivery Date, Shipping Item Quantity, Logistics Carrier details, etc.

The non-personal data processed as part of this operation would not attract any privacy related compliance requirements. Personal data or sensitive data is not collected during this operation. Hence, this type of processing activity would not attract the regulatory requirements associated with sensitive data processing in India such as data residency.

4. Invoicing and Payment

Organizational payment and invoicing processes for tracking and execution of on-time payment as well as working capital management. A typical supplier invoice management process would involve these activities: Supplier Invoice Generation, Supplier Invoice Validation (2/3/4-way matching), Invoice Posting, Invoice Clearance, Payment Acknowledgement.

Figure 7: Process Flow and Architecture



Source: Author, on the basis of stakeholder consultations

Data collected and used during this process consists of non-personal data such as Supplier Invoice number, Supplier Invoice Date, Supplier GST number, GST Invoice, Payment Method, Payment Details - Transaction Reference number, Payment Details - Transaction Date, Withholding Tax, Claims/ Deductions, etc.

The Non-personal data processed as a part of this operation would not attract any privacy related compliance requirements. Personal data or sensitive data is not collected during this operation. Hence, this type of processing activity would not attract the regulatory requirements associated with sensitive data processing in India such as data residency.

C

Security Considerations

The enterprise's decision makers must evaluate the security safeguards guaranteed by the service provider and the possibility of exercising proportionate control over the service provider through security monitoring and reporting to stay abreast with the changing risk landscape.

Security of data on the cloud is indeed one of the most important considerations for enterprises. This section captures various technical and regulatory measures that are currently existing in the ecosystem with the objective of addressing the data security concerns on the cloud. Starting with the guidance and recommendations made available by the regulatory and policy making bodies, this section moves on to the key technological aspects of cloud security.

For many of the enterprise's information risk leaders, the main risks of cloud computing are seen to be in maintaining resilience and control of the technology environment, security and data management. Yet these fears can be misplaced, since cloud also promises to reduce risks in each of these areas if service selection and adoption are planned with care. At the same time, outsourcing workload to the cloud does not outsource responsibility of risk.

Security regulatory landscape for public sector enterprises

The National Critical Information Infrastructure Protection Centre (NCIIPC) has issued guidelines/ best practices for public sector critical information infrastructure to maintain a high security posture [25].These guidelines are as follow:

I. Ensure that cloud provider is using strong encryption methods.

II. Data backup must be managed by the organization/enterprise itself.

III. There must be barriers to keep critical information separate from other information and organizations.

IV. Cloud-Organization and Cloud-Cloud interlinkages must be secured.

V. Identity and Access Management: It should be ensured that the information data is accessible to authorized users only.

VI. Logs at provider's end should be maintained and stored in encrypted form. Access to logs must be limited to only a few persons.

VII. Security related issues /aspects may be covered under Service Level Agreements (SLA). As a rule, access to critical information should be minimum, particularly from mobile endpoints.

VIII. There should be a breach reporting mechanism for any security related incident not only in the data that the provider holds for the subscriber but also the data it holds about the subscriber.

IX. Client side and server-side systems must be protected by timely updating, patching etc.

X. Access to information, network services, operation system, application and system should be controlled.

Under the Meghraj Cloud Policy, there are specific requirements for CSPs, which are offering cloud services to government/public sector organizations. Although no comprehensive laws or requirements are in place at this stage. The National Cyber Security Policy 2013 mentions the need to comply with global security standards.

However, according to the latest Ministry of Electronics and Information Technology (MeitY) guidelines, CSPs need to consider the following security standards.

I. ISO 27001 - Data Center and the cloud services should be certified for the latest version of the standards.

II. ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology.

III. ISO 27018 - Code of practice for protection of personally identifiable information (PII) on public clouds.

IV. ISO 20000-9 - Guidance on the application of ISO/IEC 20000-1 to cloud services.

V. PCI DSS - compliant technology infrastructure for storing, processing, and transmitting credit card information on the cloud – This standard is required if the transactions involve credit card payments.

MeitY with the help of Standardisation Testing and Quality Certification (STQC) carries out the audit and is in the process of certifying the service offerings of CSPs for the above-mentioned standards. MeitY suggests that the respective organizations include the following clauses in their agreements:

1. The CSP shall comply or meet any security requirements applicable to CSP published (or to be published) by MeitY or any standards body setup/recognized by the Government of India from time to time and notified to the CSP by MeitY as a mandatory standard.

2. The CSP shall meet all the security requirements indicated in IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply to the audit criteria defined by STQC (The Departments may refer to the Information Classification, National Information Security Policy, and Guidelines, Ministry of Home Affairs (MHA) while choosing to deploy cloud computing).

Salient Security Practices and Measures

Data Encryption and Protection on Cloud

I. Measures need to be taken proactively in order to secure data on the cloud. Need for adequate and robust data encryption has been like never before. Typically cloud service providers offer encryption services – ranging from an encrypted connection to limited encryption of sensitive data – and provide encryption keys to decrypt the data as needed.

II. Cloud cryptography is another way to secure cloud computing architecture. Providers typically employ cryptography to offer a layer of information security at a system level and enable secure access to whoever needs shared cloud services. This layer of encryption is based on the Quantum Direct Key System, which is an advanced system of symmetric encryption keys. Users receive a public and private key pair with a specific ID. Cryptographic cloud computing can also minimize network congestion.

III. Many cloud providers offer encryption services to safeguard the client's data when using their cloud storage. Local encryption will offer an extra layer of security because decryption is necessary before accessing the files or data. Encrypting data at rest is great, but encrypting data in transport is even better.

Identity and Access Management

I. Having a robust Identity and Access Management Strategy for cloud environment is imperative to automate risk protection and authenticate each and every user requesting access to the resource.

II. In line with the philosophy and thinking of zero trust architecture, users should only be able to get access to the resources they need in order to accomplish the task at hand. Context-aware access is pivotal to a granularized approach to IAM. Granular access control policies help ensure that the requisite security controls are in place while access is being given to various cloud resources.

III. Also, IAM is instrumental in keeping identity-based attacks and data breaches at bay. In today's era when remote working has found a special and perhaps permanent place in the corporate ecosystem, IAM systems have become more important.

Cloud Security Monitoring

I. Effective cloud monitoring presents an easier way to identify patterns and highlight potential security vulnerabilities in cloud infrastructure. Visibility forms an integral part of the underlying objectives and perhaps challenges of Cloud Monitoring. There exist several approaches to achieving cloud security monitoring – it could be on the cloud platform itself, on premises or by leveraging a third-party cloud provider.

II. Effective cloud monitoring solutions can scan, evaluate, and classify data before it's downloaded to the enterprise network, avoiding the introduction of malware and other malicious elements that can create vulnerabilities and leave the enterprise open to data breaches.

D

Contractual Considerations

Public sector enterprise decision makers must evaluate the contractual guarantees and safeguards offered as part of the engagement with the cloud service provider. The decision makers must also gauge the competence of the service provider to uphold the said regulatory or legislative compliance requirements.

Applicable Law and Jurisdiction

Data is subject to the laws of the country in which it is stored. However, the data processor and data controllers are subject to the laws of the country in which they received the data from the data subjects. Laws from other jurisdictions could apply to the data, depending on a set of scenarios, which are evolving through domestic and international precedents. Compliance with Data Protection regulations is a fundamental requirement for all cloud-based solution service contracts.

Security Safeguards

The enterprise must ensure that the solution provider has adequate technical and legal measures in place to protect the data, and these measures must be proportionate to the nature of the data being processed and stored. The personal data must be secure from accidental loss, damage and destruction.

Sub-contracting

Enterprises should be in the know about any third parties that will have access to their data and for this reason, the extent and nature of the supply chain. The public sector enterprise must see to it that the cloud-based solution provider's liability for sub-contractor failure is included.

Rights and Responsibilities

The contract should clearly reflect the rights and responsibilities for both parties. The enterprise should have a thorough understanding of the respective responsibilities and how risk is being apportioned.

Audit Rights

Enterprises in most instances push for contracts with service providers to contain clauses to enable the right to audit the service provider. Some consider it necessary to ensure the providers' contractual and statutory compliance, on top of ensuring that the enterprise's information assets are being processed and stored in accordance with the terms of the contract. An enterprise may want to invoke audit rights in the event of events such as a data breach.

Service Level Agreements

Most service providers offer some form of service level agreements, which may not be as comprehensive as those that the public sector enterprise might expect under a typical IT outsourcing contract. Usually, service level agreements tend to be standard and non-negotiable. The onus is on the enterprise to select a service level regime which meets the needs of the organization.

Conclusion: Key Considerations

This paper examined the enterprise's concerns around security, privacy and local storage. It provides a short guide for decision makers who are accountable for information risk and other senior personnel who need to make proportionate and risk-aware choices when considering the purchase of cloud services for enterprise use. One of the areas of uncertainty at the time of writing this paper are the requirements with respect to the Indian Personal Data Protection Bill, 2019, which may be subject to change in the future. The key considerations that require in-depth evaluation are as follows:

01 Assess data usage

Evaluate the category of data being processed as part of the service offering and the associated regulatory requirements such as local storage, etc.

02 Evaluate accountability measures

Evaluate the capability of the service provider to meet compliance requirements and the existence of established practices to showcase accountability.

03 Evaluate terms of service

Evaluate the contractual guarantees and safeguards offered as part of the engagement with the cloud service provider.

04 Assess security safeguards

Evaluate the security safeguards guaranteed by the service provider and the possibility of exercising proportionate control over the service provider through monitoring and reporting.

05 Assess compliance capabilities & support

Evaluate the competence of the service provider to meet the applicable regulatory or legislative compliance requirements.

06 Assess privacy maturity

Evaluate the overall privacy posture of the service provider and the existence of established practices to assist the enterprise in meeting the privacy expectations of the individual.

Frequently Asked Questions

1 What category of data requires local storage within India as per the Personal Data Protection Bill, 2019?

Clause 33, PDP, 2019 specifies that SPD may be transferred outside of India but must continue to be stored in India. In effect, a local copy of all SPD must remain within India at all times. Clause 33 further notes that critical personal data may only be processed in India. "Critical personal data" is not defined in the bill, it would be notified by the central government at a later stage. *Read more: Section 'Personal Data Transfers and Local Storage', Pg. no. 10.*

2 Are there any local storage requirements associated with personal data as per the Personal Data Protection Bill, 2019?

There are no restrictions on storage and transfer of personal data outside India. *Read more: Section 'Personal Data Transfers and Local Storage', Pg. no. 10.*

3 Are there any local storage requirements emerging from any other regulatory directives or guidelines for public sector enterprises?

There are no local storage requirements emerging from any other regulatory directives or guidelines from the National Critical Information Infrastructure Protection Centre (NCIIPC).

4 What regulatory guidance is available for the Public Sector Enterprises to ensure Security of workloads on the cloud?

The NCIIPC has issued guidelines/best practices for public sector critical information infrastructure to maintain a high security posture. The Ministry of Electronics and Information Technology has issued guidelines for cloud service providers, stating the security standards that need to be considered by the CSPs. MeitY with the help of Standardisation Testing and Quality Certification (STQC) carries out the audit to verify their presence. *Read more: Section 'Security regulatory landscape for public sector enterprises', Pg. no. 16.*

5 What are the key aspects that enterprises should factor in from Security and Data Protection standpoint while drafting contracts with the CSPs?

MeitY suggests that the respective organizations include the following clauses in their agreements:

- The CSP shall comply or meet any security requirements applicable to CSP published (or to be published) by MeitY or any standard body setup/recognized by Government of India from time to time and notified to the CSP by MeitY.
- The CSP shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply with the audit criteria defined by STQC (The departments may refer to the Information Classification, National Information Security Policy, and Guidelines, Ministry of Home Affairs (MHA) while choosing to deploy on the cloud).

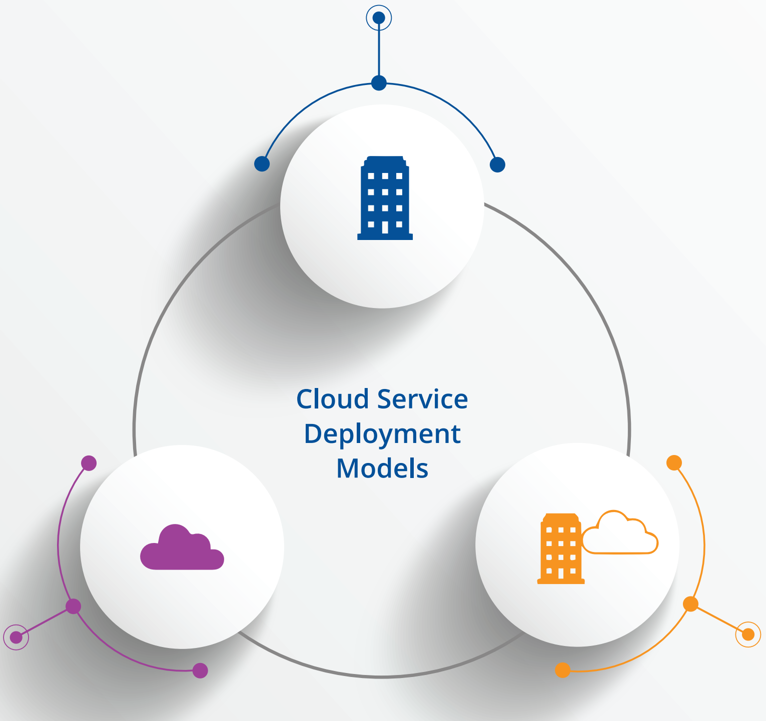
6 Would the STQC certification be required if the solution is not using any personal data/ sensitive data??

STQC certifications/audit requirements are applicable to cloud service providers offering services to any government or other government departments. CSPs are expected to provide and implement security mechanisms for handling data at rest and in transit. This covers all the data types, whether non-personal, personal or sensitive data.

Appendix 1
Types of Cloud Service Deployment Models

Private Cloud

The Cloud infrastructure is dedicated to an organization which may be managed by the organization itself or a third party, and may exist on the premises or off them.



Cloud Service Deployment Models

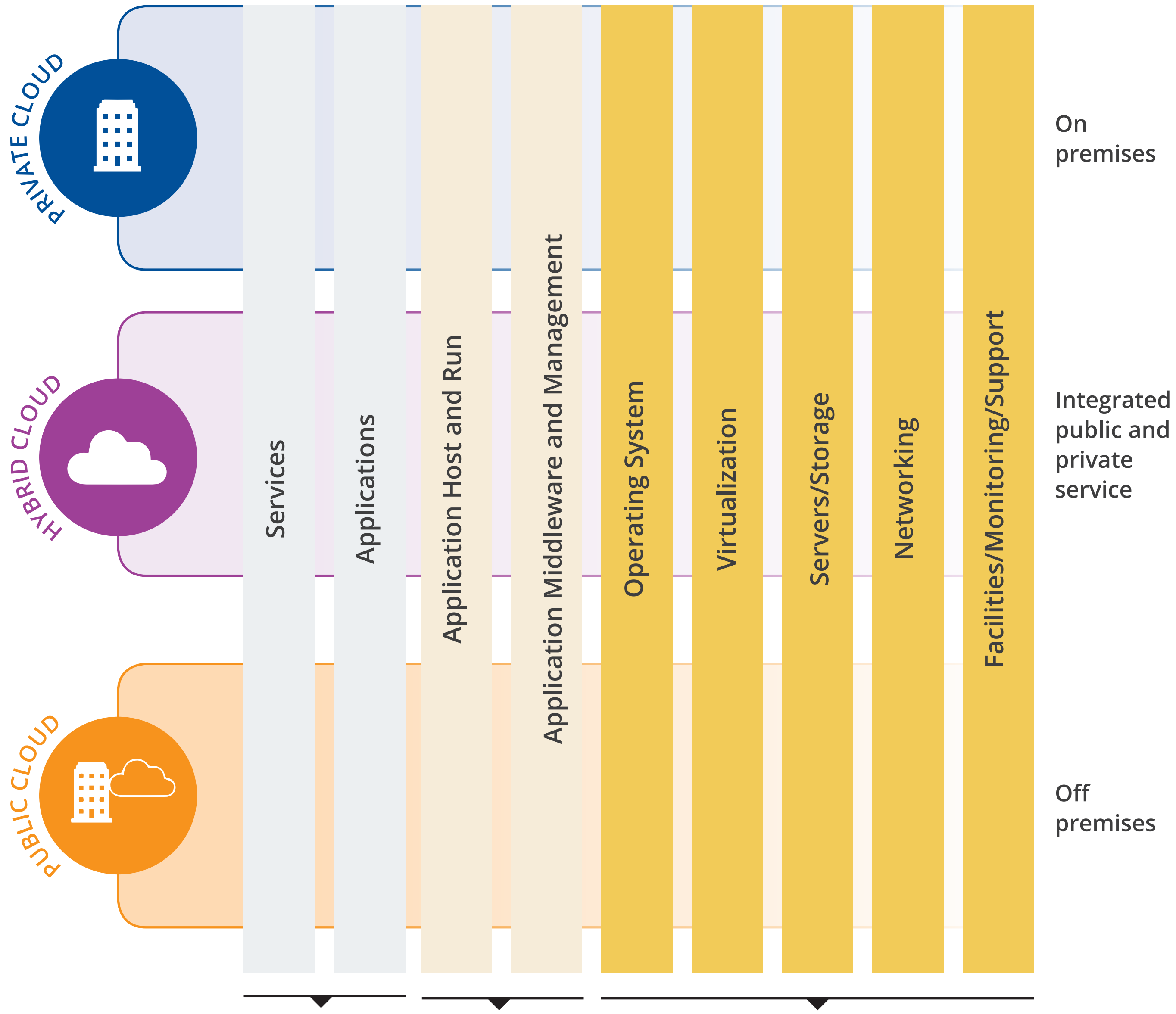
Hybrid Cloud

It is a composition of two or more Clouds (private on premise/off premise, or public) that remain unique entities, but are bound by standardized or proprietary technology that enables data and application portability.

Public Cloud

The Cloud infrastructure is made available to the general public or enterprises while it is owned by a third-party Cloud Services Provider.

Appendix 2
Types of Cloud Service Models



Softwareas a-Service (SaaS)
Software that provides a purpose-built business service to the client.

Platform-as-a-Service (PaaS)
Ready-to use scalable, integrated app & data hosting.

Infrastructure-as-a-Service (IaaS)
Horizontally and vertically scalable of compute, storage and networking delivered to an application on-demand.

References

1 NASSCOM, “Cloud: Next Wave Of Growth In India 2019”, Available at: https://nasscom.in/knowledge-center/publications/nasscom-cloud-next-wave-growth-india-2019 (Last accessed: 6 September 2021)

2 KPMG, “Moving to the cloud: Key considerations”, (2021) Available at: https://assets.kpmg/content/dam/kpmg/pdf/2016/04/moving-to-the-cloud-key-risk-considerations.pdf (Last accessed: 18 June 2021).

3 Personal data is information that relates to an identified or identifiable individual. What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors. If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

4 Rule 3, Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to;— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

5 Data controllers are entities who are in charge of determining the means and purpose of processing personal data.

6 Data processors are entities who process personal data on behalf of/under the instructions of a data controller.

7 Clause 3(14), Personal Data Protection Bill, 2019, ‘Data principal means the natural person to whom the personal data relates.’

8 Clause 3(13), Personal Data Protection Bill, 2019, ‘Data fiduciary means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data’.

9 Clause 26, Personal Data Protection Bill, 2019. Classification of data fiduciaries as significant data fiduciaries is based on the following factors: (a) volume of personal data processed; (b) sensitivity of personal data processed; (c) turnover of the data fiduciary; (d) risk of harm by processing by the data fiduciary; (e) use of new technologies for processing; and (f) any other factor causing harm from such processing.

10 Dr. Ann Cavoukian, Privacy by design: 7 foundational principles, (2021), Available at: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (last accessed: 18 June 2021).

11 Clause 17(1), Personal Data Protection Bill, 2019.

12 Clause 17(3), Personal Data Protection Bill, 2019.

13 Clause 19(1), Personal Data Protection Bill, 2019.

14 Clause 19(1)(a), Personal Data Protection Bill, 2019.

15 Clause 20(1), Personal Data Protection Bill, 2019.

16 Clause 20(2), Personal Data Protection Bill, 2019.

17 Clause 18(1), Personal Data Protection Bill, 2019.

18 Clause 18(4), Personal Data Protection Bill, 2019.

19 Cloud standards customer council, “Data residency challenges”, (2017) Available at: https://www.omg.org/cloud/deliverables/CSCC-Data-Residency-Challenges.pdf (Last accessed: 18 June 2021).

20 Cloud standards customer council, “Data residency challenges”, (2017) Available at: https://www.omg.org/cloud/deliverables/CSCC-Data-Residency-Challenges.pdf (Last accessed: 18 June 2021).

21 Clause 33, Personal Data Protection Bill, 2019.

22 Clause 3(36), Personal Data Protection Bill, 2019.

23 Clause 33(2), Personal Data Protection Bill, 2019.

24 Clause 34, Personal Data Protection Bill, 2019.

25 NCIIPC, “Guidelines for the Protection of National Critical Information Infrastructure”, (2015) Available at: https://www.asianlaws.org/gcld/cyberlawdb/IN/guidelines/NCIIPC_Guidelines_V2.pdf (Last accessed: 18 June 2021).

26 Meity.gov.in., “National Cyber Security Policy”, (2013), Available at: https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf (Last accessed: 18 June 2021).

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

DATA SECURITY COUNCIL OF INDIA

NASSCOM CAMPUS, 4th Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

For any queries, contact:

E: info@dsci.in | W: www.dsci.in

DSCI_Connect dsci.connect dsci.connect data-security-council-of-india dscivideo