Personal Data Protection and Data Localization

Rethinking Your Enterprise Multi-Cloud Strategy

By Nitin Mishra
SVP & Chief Product Officer,

In the wake of the Facebook – Cambridge Analytica data scandal in the US and the implementation of GDPR across Europe, the Government of India has been actively working towards bringing strong legislation that protects personal information. In this regard, the government has recently taken two giant steps:

- In July, it submitted the draft 'Personal Data Protection Bill, 2018' to the Ministry of IT. The bill is intended to provide protection of data privacy and covers areas such as data collection, processing, storage, quality, accountability, portability, purpose, consent and Right to be Forgotten
- It also proposed data localization in August – which means that personal critical user data of Indian citizen (or entities), as well as any data generated in India, should be stored and processed in India itself. This is intended to help investigative agencies access data easily, in case of breaches or illegalities.

These two steps are expected to have significant repercussions, not just for organizations and their IT departments, but also for companies that store, process and manage personal data – such as Cloud Service Providers (CSPs), MSPs, third-party data centers and hosting service providers,

As these policies come into force, the impact to enterprise IT teams would, in all probability, be significant, considering the fact that most large organizations today already use a diverse spectrum of cloud-based applications, platforms and infrastructure. Generally termed as 'multi-cloud' organizations often do not have significant control on how cloud resources are accessed and provisioned by various departments and teams. Organizations, as a result, end up with an unstructured and diverse data footprint, often extending across platforms, applications and geographies. Here are six important aspects of a multi-cloud strategy that will help CIOs adhere to regulation around personal data privacy and localization.

1. CREATE AN ENTERPRISE POLICY FOR PERSONAL DATA ON THE CLOUD

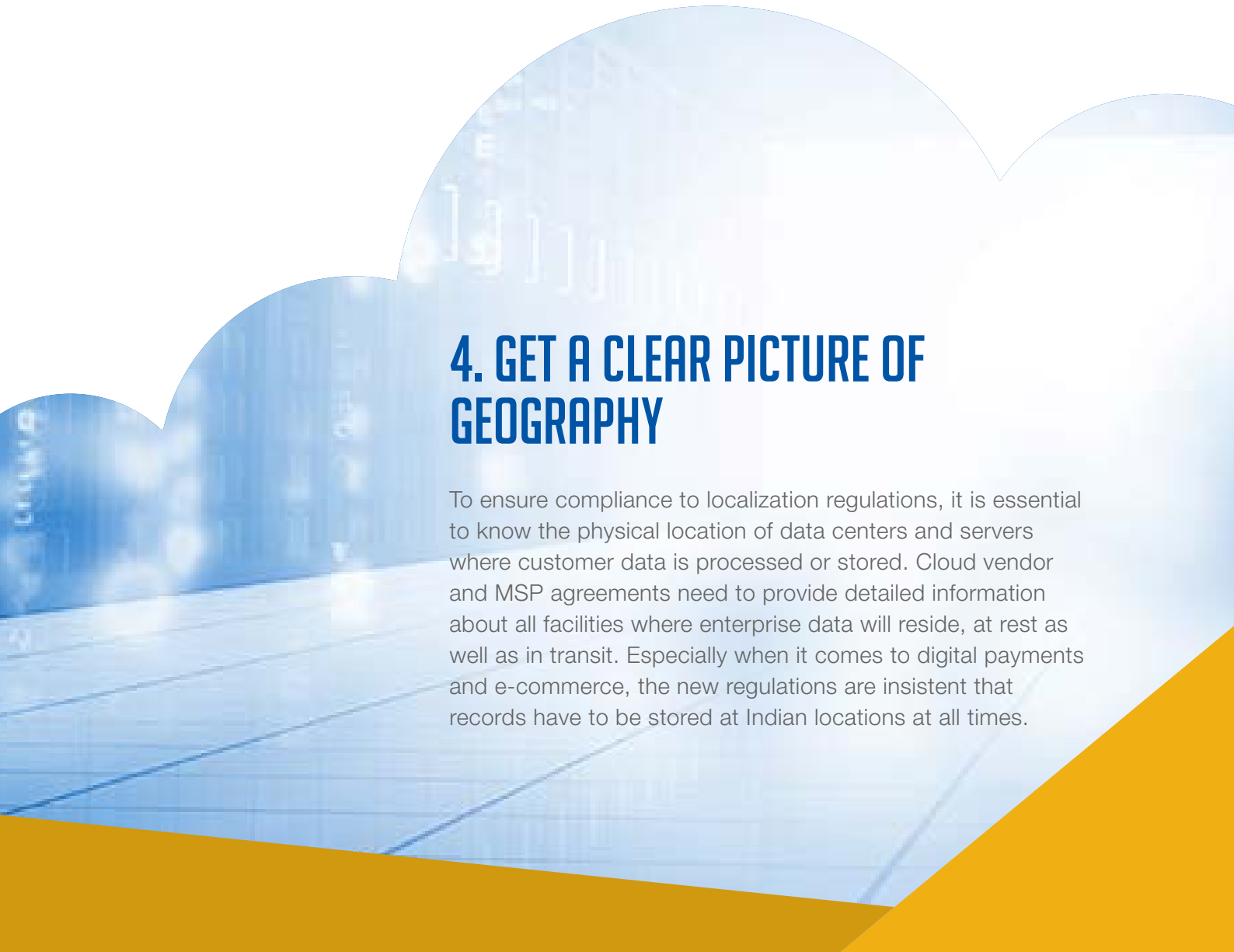
Enterprise IT and security teams (sometimes companies have separate teams for regulatory compliance, data protection, information risk management, etc.) not to enforce a strong policy for uploading, storing and processing data on any resource outside the organizational firewall (e.g. mobile devices, apps, SaaS tools). Policies need to be include access control mechanisms and adequate checks and balances to prevent cases of inadvertent non-compliance. This is particularly true for industries such as IT, banking, hospitals, insurance, financial services and telecom, which generally store a large amount of sensitive personal data (such as financial status, health conditions, product preferences, etc.)

2. MAP WORKLOADS TO INFRASTRUCTURE TYPES

Companies need to make a clear distinction between public and private workloads. In a multi-cloud setting, IT teams must put in place access management and security protocols to ensure that specific workloads are always mapped to allocated resources. For example, personal critical data must always reside on private cloud infrastructure in an India-based datacenter. Not –critical information, such as usage analytics, population demographics, reports, dashboards, etc. can be stored in cloud infrastructure or hosted service providers outside India. In many cases, organizations may choose to use de-identified customer data for analytics and statistical modelling.

3. NOMINATE AND AUTHORIZE 'DATA STEWARDS'

Data governance and privacy needs to be a formalised process within the organization, and needs organization-wide buy-in, at all levels. Getting your data privacy setup necessarily involves extensive change management initiatives that involve people, processes and technology enablers. Globally, organizations that have high levels of data maturity have leadership roles around data quality management, data governance and personal data protection. In the Indian context, organizations may start with appointing 'data stewards' who have the authority to identify and act on incidents of data breach. This should be backed by formal data reconciliation and CAPA (Corrective Action Preventive Action) mechanisms which ensure that similar data breaches do not occur in the future.



4. GET A CLEAR PICTURE OF GEOGRAPHY

To ensure compliance to localization regulations, it is essential to know the physical location of data centers and servers where customer data is processed or stored. Cloud vendor and MSP agreements need to provide detailed information about all facilities where enterprise data will reside, at rest as well as in transit. Especially when it comes to digital payments and e-commerce, the new regulations are insistent that records have to be stored at Indian locations at all times.

5. BUILD AUTOMATED MECHANISMS TO MANAGE 'CONSENT'

The way GDPR has been enacted shows us that 'consent' will play a critical role in data privacy compliance. In the present draft Personal Data protection Bill, the word 'consent' appears 36 times. The act covers the meaning of consent in great detail – covering aspects like meaningfulness, clarity of scope, freedom, ease and ability to be withdrawn. The act also includes extensive clauses around the 'Right to be Forgotten', where the owner of the data has 'the right to restrict or prevent continuing disclosure of personal data', subject to withdrawal of consent.

6. PARTNER WITH AN INDIAN DATACENTER

With data localization norms coming into effect, many of the global cloud service providers will find it challenging to service Indian customers cost effectively, since they will need to set up dedicated cloud facilities in India. However, cloud leaders such as Netmagic have already built huge operational volumes in India. This makes it easy and highly cost effective for organizations to move their workloads to India based datacenters. Also, as an NTT Communications company, Netmagic is very strongly positioned to provide world-class cloud hosting, network and storage services, in a compliant, secure and high performance environment.

Of course, there are many grey areas that have not yet been thought through. For example, applying the data localization laws on SaaS based enterprise software vendors (portals, e-commerce sites, mobile apps) outside India that have their own contractual terms and data privacy policies with end users. Would data entered into an application with servers in Singapore be considered as 'data generated in India'?

While legislature evolves to address such current and future challenges, organizations embarking on a multi-cloud journey have some time to put adequate processes and policies in place, deploy robust cloud management and data governance tools and work towards a single, unified data privacy policy across all IT resources across the enterprise – including on-premise, cloud-based, hosted and third-party infrastructure providers.