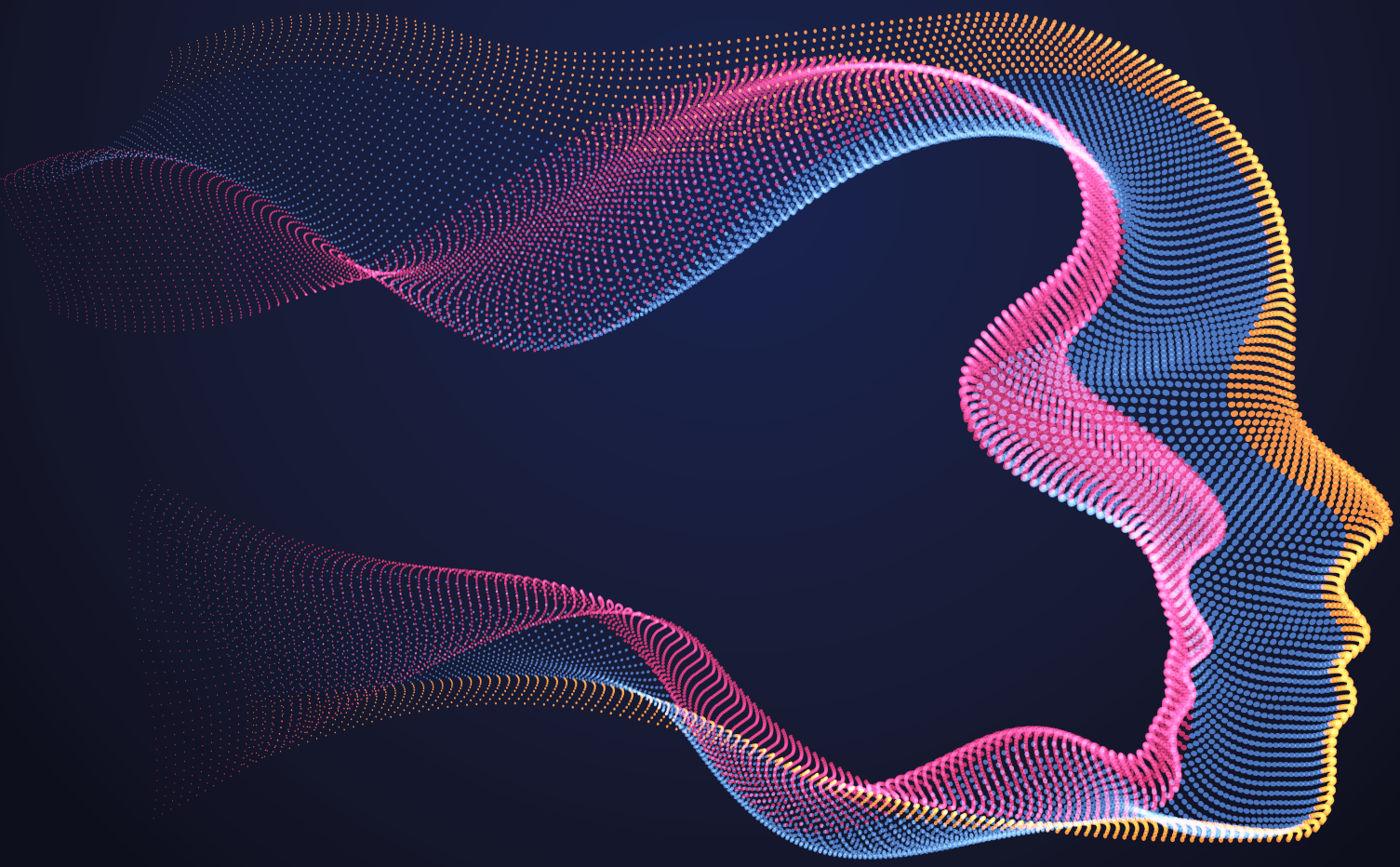
TECH mahindra

Whitepaper

The NXT Road to Global Data Residency



Abstract

Data Residency has taken a center stage with 137 countries out of 194 countries passing the data protection and privacy laws. Interpreting applicability of these **cross border and cross regulatory laws** is a complex job which financial services firms have to handle with dexterity. This paper outlines what data residency is, the contours of data residency covering storage, access, security, privacy; and the risks posed to the financial services firms and actions needed to meet these guidelines.

Decision makers from the banking and financial services (BFS) industry can utilize this whitepaper to understand a technology-agnostic and practitioner's view.

Key Takeaways

- Emerging landscape of data residency regulations and need for compliance by financial services firms
- Three step holistic framework for meeting the data residency regulations
- Mapping template for the risk classified data with core focus on "portability of the data, on building highest security of customer controls and segregation of roles and responsibilities"

Introduction

It is a universal truth that the modern world is awash with data. Data has become the **fuel** that provides **insight** into central economic activities of **people**, **business**, and **governments** across the globe. The financial services firms once were considered as the **physical money custodians** and their liability was limited to the value of money deposited with them. But with digitalization the amount of diverse data held by the customers is large and financial services firms are referred to as **digital data custodians.** The winds of change are paving the way for more data creation powered by proliferation of internet, ability to capture data from IOT and sensors, launch of 5G and falling data storage costs which has led to an exponential growth in new data created.

Based on customer transaction data, financial services firms would be able to predict customer needs and customize their offering to match the needs of the customer (see Figure 1).

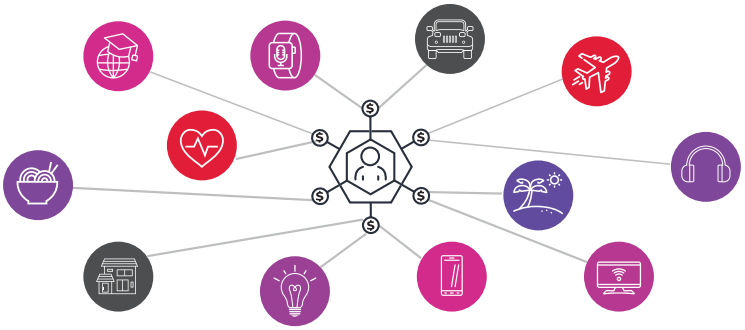


Figure 1: Generation of Contextual insights based on transaction data

By 2025 it is estimated that that the world data will grow to 175 Zetta bytes. In this context financial services firms have a larger responsibility to ensure safety of data of their customers at all touch points. Cybercrime is expected to reach $10.5 trillion by 2025.

Current state and need for data residency

Around the world, sovereign nations are promoting data localization regulations covering data privacy and protection. 137 out of 194 countries have passed data protection and privacy laws. These rules are making companies to rethink and alter their data management approach. This change comes at a huge cost as financial services firms lose economies of scale from having dedicated single large infrastructure setup to moving to multi geo infrastructure setup. The compliance costs also spiral up as each geo is a separate instance having people with the same skills implementing the guardrail for each of the geography. In North America it is estimated that the cost of meeting the 50 new state privacy laws in the next 10 years can cost $1 trillion.

Localization laws are intended to protect the data of its citizens, prevent cybercrime, promote local economy and talent. Data is a state subject. A deep dive into the data residency laws clearly call out where can the data be stored, how it must be stored, who are allowed to access the data etc.

Customer views:
In a recent conversation with a MNC bank, the CISO expressed concerns in meeting the data residency laws in 60 countries they operate

Annual report:
In a study conducted by Tech Mahindra into the annual reports Credit Suisse, Citi, Standard Chartered, HSBC have highlighted data residency as a **"key risk."**

Tech Mahindra - Data Residency Framework

Financial services firms need to look at the data residency laws from the lens of the regulator to understand the **motives**. The intent of the regulator on data privacy and security needs to be met by the financial services firms. In this thought paper we have proposed a three-step framework (see Figure 2) that can be adopted by the financial services who are wanting to comply with the data localization laws.

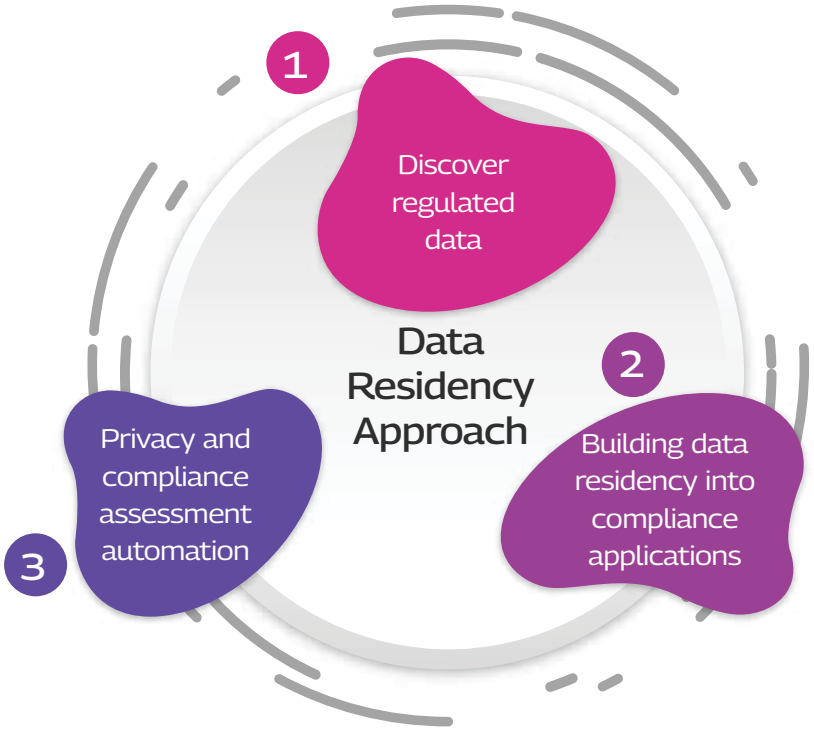


Figure 2: The three-step framework by Tech Mahindra

1.Discover regulated data
2.Building data residency into compliance applications
3.Privacy and compliance assessment automation

The data residency approach is a matured framework, which has been validated with analysts, financial services firms, and OEMs. **As the initial step**, the three-step framework proposes data discovery to identify and segrgate regulated data and non regulated data. This step is a herculean task as various data repositories need to be identified and evaluated. This is also a dynamic step as it is a continuos process in evaluating and segregating data generated being shared on a continuos basis. In some data residency bills the criteria mapping of data changes from one geography to the other geography.

In the second step, the compliance regulations have to be built into the applications. It is a key stage where the data residency laws clearly call out the actions on **data storage, data processing,** among others. Understanding and interpreting the data laws and proposing the guardrails for privacy and security are critical. The more number of geographies the financial services firms operate the more number of laws to be evaluated and regulations to be complied.

The third step proposes building an automated compliance dashboard with a detailed view of the compliance checklist that can be monitered by the board and by the compliance team. This is a key step as liability in non compliance to the data residency laws can cause huge financial loss. This can be used as a barometer to understand the current compliance status.

Steps to Achieve Data Residency

1. Discovering the regulated data :

Data is heterogeneous and, in this form, can't be inferred to any person or an institution. But when combined with other data can make a world of impact. The data residency laws address this key issue by classifying the data.

They key to compliance would be segregating the regulated data like personally identifiable information (PII) and other forms of sensitive data. Organizations must take a pragmatic approach as there are varied repositories of data and data can be in structured or unstructured format.

Proposed approach:

1. Define what are classified as regulated data points by decoding the laws
2. Identify the sources which hold the regulated data
3. Build machine learning models which can connect with the sources systems and identify the regulated data from them. Financial services firms can also leverage machine learning (ML) models created by system integrator to fasten this journey; and these models are matured
4. Classify the data points into PII/ sensitive and non-regulated
5. Assign risk rating to the classified data as high, medium, and low risk
6. The assessment needs to be a continues one.

By the end of this phase customer would have a clear understanding of the regulated data and risk exposure he is subject to.

Sample classification is enclosed below for ready reference.

Personal data
These are the data points based on which an individual can be identified. Name, date of birth, email, sex, address, social security number, pin code, bank account details, credit card info.
Note: Data identified under this head is classified as High Risk

Proprietary data
These data points cover the intellectual property assets of the firms and are used extensively in day-to-day management. Ex: IPs, M&A data, unpublished financial data, reports to regulator, core formulas for risk management, loans.
Note: Data identified under this head is classified as Medium Risk

Public data
These data points are published information from financial services firms. Ex: Published annual report, account opening form, new product launches.
Note: Data identified under this head is classified as Low Risk

2. Building compliance regulations

After having classified the data a further deep dive into data residency regulations clearly call out the guardrails for data security and privacy controls covering data storage and access. The global privacy laws like General Data Protection Regulation **(GDPR),** Digital Operational Resilience Act **(DORA)**, and the **local laws** clearly spell out that the financial serviced firms are the owner of the data. The intention of the regulators is to always protect data with highest safety and privacy controls.

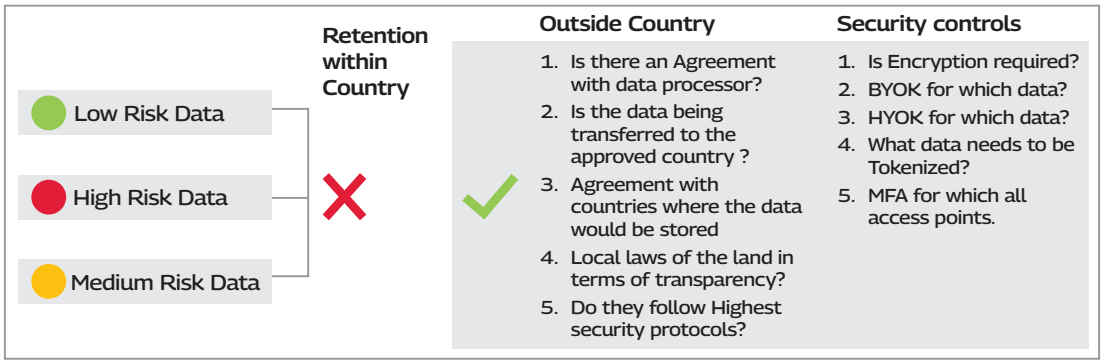


Figure 3: A sample guardrails list which majority of the laws call for

The approach of the financial services firms could be to host data in their own data center, move it to a private cloud or a public cloud. Depending on the place of hosting the guardrails protocols vary. Ex: One of our financial services firms in Europe migrated to a public cloud which was hosted in the country. We worked with the customer in ensuing that the data when transferred to the cloud was encrypted at all times, the encryption keys were owned by the client, i.e., **bring your own key (BYOK)** and not provided from the cloud hyperscaler. The client further strengthened his security protocols by ensuring the keys for access to the IT environment were stored in the client's environment i.e., **hold your own key (HYOK)** and not on the cloud.

Before finalizing the approach for data storage and security controls the financial services firms can create a detailed checklist and map them based on **complexity of data portability, how to increase security protocols based on data risk,** and **segregation of duties with suitability. See Figure 4.**

Sample mapping sheet

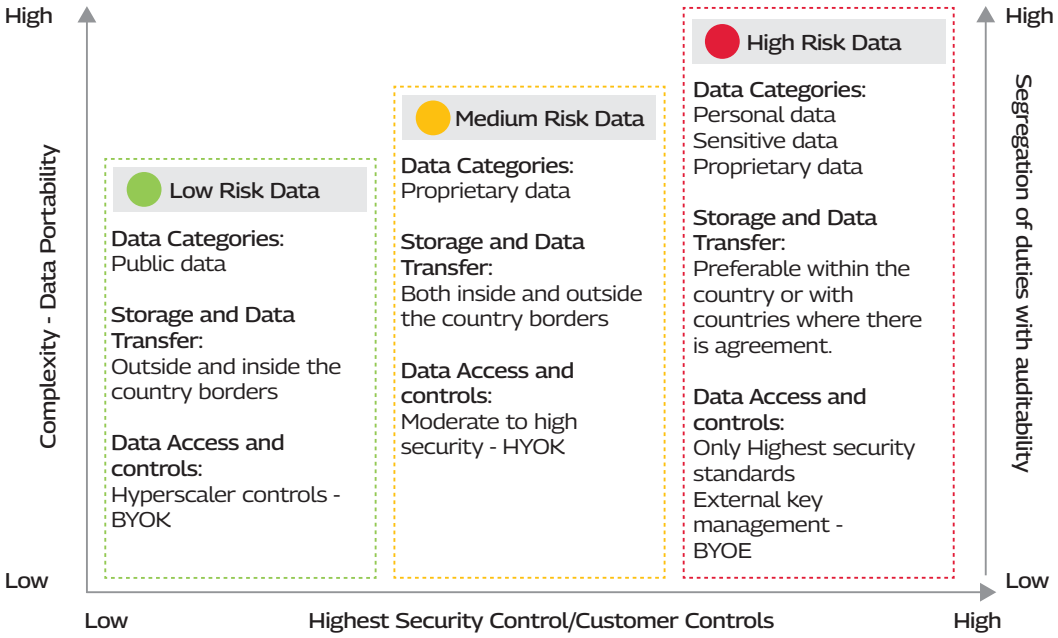
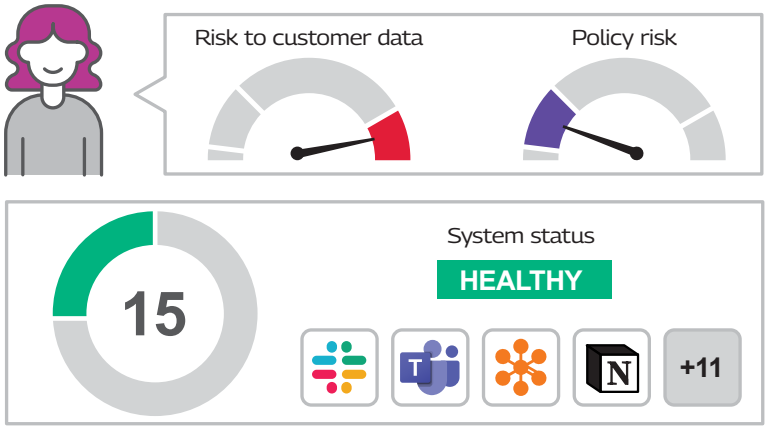


Figure 4: An example of how firms can map data approach and build compliance standards

3. Automating privacy and compliance assessment

Till now there have been 311 GDPR fines[1] imposed across the world. Some of the prominent reasons are

- Insufficient security of systems and servers that are used for processing personal data
- Failure to notify the commissioner on data breach
- Insufficient technical measures to ensure information security
- Inadequate basis for legal processing of personal data



Financial services firms are subject to both external audits and internal audits covering global privacy laws and local laws. The implications of non-compliance to these laws can be catastrophic to financial services firms. To overcome this financial services firms can create an automated monitoring environment for the compliance laws they are subject to. For our customer, we built an automated GDPR monitoring environment which clearly calls out the actions and the sub-components for the actions with status update.

Audit parameter	Compliant	WIP	Non-compliant
Accountability governance			✗
Processing principles		☐	
Privacy by design and default			✗
Data protection and impact assessment			✗
Records of processing	✓		
Data subject rights	✓		
Consent and notice			✗
Breach management	✓		
Processors		☐	
Data transfers	✓		

Tech Mahindra for your Data Residency Journey

Tech Mahindra brings in a matured offering to address the fragmented data residency regulations in a systematic way. The approach is enriched by

- Conducting an end-to-end assessment of the data residency laws, mapping them and aligning them to the guardrails of the residency laws
- Understanding the potential risks for each data type in a country, leveraging the existing infrastructure and suggesting a viable economic solution
- Undertaking data localization by migrations of data-to-data centers or cloud
- Enabling privacy and security protocols when transferring the data. For example, field level encryption, BYOE, HYOK
- Working with the organizations legal counsel, internal architectural teams and security teams

References

1. GDPR Fines | A comprehensive database of GDPR fines. (n.d.). GDPR Fines - INPLP. https://gdpr-fines.inplp.com/

Authors

Lakshmi Kanth

Principal consultant, banking and financial services

Lakshmi Kanth has more than two decades of experience in the banking and financial services domain. He is passionate about creating purposeful and innovative solutions for the BFSI vertical. The solutions like "RITA", "CTEE" and "data residency as a service" were unique and stood out at the time of launch. His deep domain skills and ability to map an outcome are his strengths.

Email: lakshmikanth.kurra@techmahindra.com

William Eliah

Presales and solutions lead for EMEA - data security

William Eliah has around 14 years of overall professional experience in IT and a decade of experience in the cyber security industry. He has had very successful engagements and contributions with data and databases security technologies. He is a keen learner of evolving security trends and matching relevant technologies and has a diverse and rich background with exposures to OEM and global system integrators.

Email: william.eliah@techmahindra.com