International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

Data Privacy - Governance

Jayant Dani
Chief Architect and Principal Consultant

ABSTRACT

Ensuring data privacy has become one of the highest priorities for enterprises, be it small, medium or big. Countries across the world have institutionalized data privacy regulations, which mandate protection of data privacy and reduce the risk of data breaches. The complex, varying and conflicting nature of the data privacy regulations, makes its implementation quite involved and expensive. In order to cope with such regulations, enterprises should revisit the incumbent data governance policies and deploy suitable solution.

This white paper provides an overview of data privacy policies, challenges posed and an approach for data privacy program via various privacy management functions.

Keywords

Data Privacy, Data Protection

INTRODUCTION

With contemporary enterprises doing business globally, enterprise's digital boundary does not necessarily match with its geographical boundary – rather, it spans over multitude of geographical boundaries. Thus, it is quite possible that an enterprise is based in country 'A', while one of its many data centers may be located in country 'B', the person whose data is being stored is a citizen of a third country 'C', and, the data needs to be shared with some business partner in a country 'D'. With such a logical spread of data, the potential for data privacy breach increases significantly. Data privacy regulations have mushroomed all over the world. These laws mandate enterprises to safeguard the privacy of information. These regulations can be geography-specific or industry-specific, or, both may apply. Further, these regulations keep getting upgraded over time and enterprises are expected to keep abreast with the latest version of the law. Sometimes, one may find opposing compliance needs, coming from different data protection laws.

Thus, one can imagine, the tremendous level of complexity of regulatory compliance created by the scenario described earlier. Therefore, enterprises need to comply with not just domestic data privacy regulations, but also the regulations from other countries.

Enterprises are increasingly in the lookout for robust, scalable and sustainable methodology that will help them comply with such stringent data protection needs.

Data Privacy Regulations Overview

Here are some examples of data protection regulations, in which, privacy of personal information plays a crucial role:

- European Union's (EU) General Data Protection Regulation (GDPR)
- Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada
- Personal Information Protection Act (PIPA) of South Korea

Some regulations are larger in scope, apply to a specific domain/business vertical, and include data protection as one of the key requirements. Some examples include:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes Oxley Act (SOX)

Legal frameworks such as EU-US Privacy Shield, Asia-Pacific Economic Cooperation (APEC), Cross-Border Privacy Rules System (CBPR) and data transfer legal agreements such as standard contractual clauses and binding corporate rules are also in place for cross border data flow.

Irrespective of company-size and industry, enterprises dealing with sensitive and personal data has to comply with these regulations.

Governed Data Privacy Management

Most enterprise, today, do have some level of data governance in place. Mature enterprises have very formal framework of governance. Other enterprises, which are still on the learning curve, are continuously adopting incremental steps along the governance journey.

In either case, data privacy must become an integral facet of an enterprise' data governance narrative. Fig 1 depicts the various ways an enterprise receives, processes and shares data and the data privacy steps it can take.

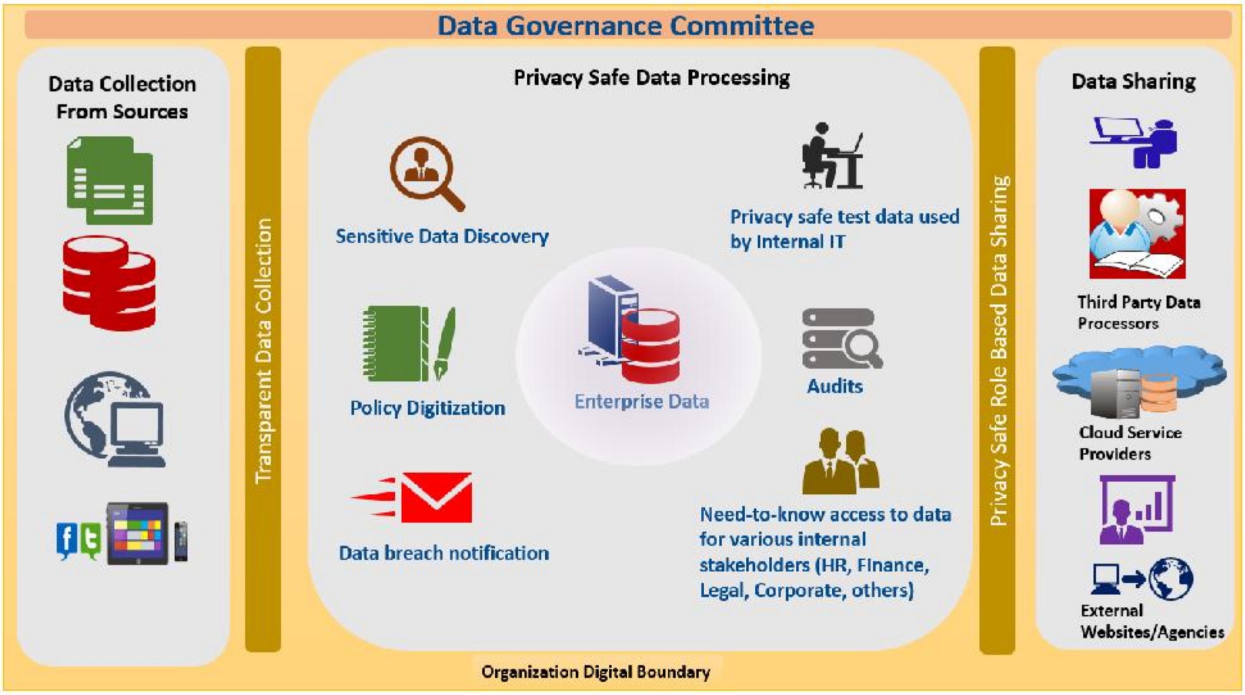

Data Governance Committee
Data Collection From Sources
Transparent Data Collection
Privacy Safe Data Processing
Sensitive Data Discovery
Privacy safe test data used by Internal IT
Policy Digitization
Enterprise Data
Audits
Data breach notification
Need-to-know access to data for various internal stakeholders (HR, Finance, Legal, Corporate, others)
Privacy Safe Role Based Data Sharing
Data Sharing
Third Party Data Processors
Cloud Service Providers
External Websites/Agencies
Organization Digital Boundary

Figure 1 Data Privacy Governance Steps

Central data privacy governance committee

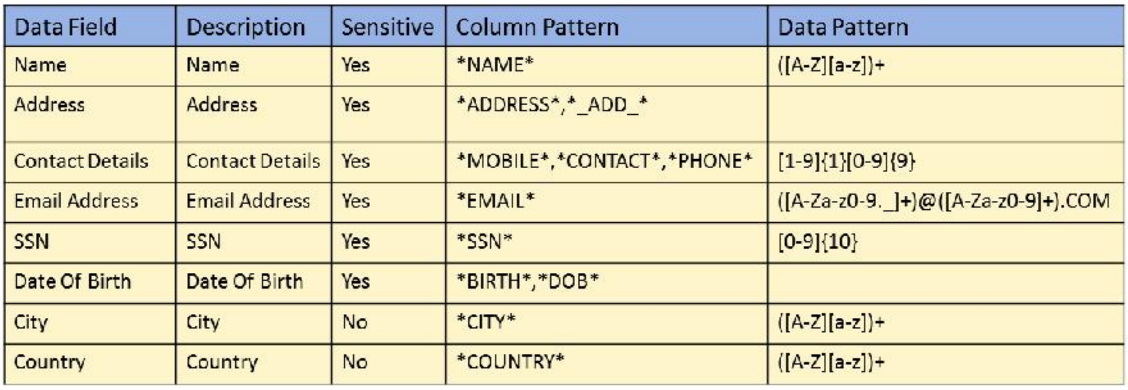
Enterprises should have central committee consisting of Chief Information Officer, Chief Data Officer and Data Protection Officer along with business stakeholders. This committee should define, enforce data protection policies and be responsible and accountable for any data privacy breach. It should revisit all existing contracts to introduce appropriate clauses for personal data processing. Also, it should observethe contracts and existing policies from time to time for compliance with evolving data privacy regulations. It should also define the compliance indices for quantitative measurement of data privacy compliance.

In parallel, it should also organize programs to spread awareness about data privacy across organization.

Sensitive data discovery

With huge volume of data being stored in data stores, enterprises should discover and classify sensitive data elements. It is strongly recommended to discover quasi identifiers as well. Enterprises should do impact and risk analysis of sensitive data processing and implement measures to mitigate the risk. Enterprise can use appropriate software for sensitive data discovery, data relationship discovery, data lineage, impact and risk assessment, which brings about some level of automation in this process.

Figure 2 shows illustrative sensitive data fields, metadata and data pattern based approaches to automatically discover the columns.



Data Field	Description	Sensitive	Column Pattern	Data Pattern
Name	Name	Yes	*NAME*	([A-Z][a-z])+
Address	Address	Yes	*ADDRESS*,*_ADD_*	
Contact Details	Contact Details	Yes	*MOBILE*,*CONTACT*,*PHONE*	[1-9]{1}[0-9]{9}
Email Address	Email Address	Yes	*EMAIL*	([A-Za-z0-9._]+)@([A-Za-z0-9]+).COM
SSN	SSN	Yes	*SSN*	[0-9]{10}
Date Of Birth	Date Of Birth	Yes	*BIRTH*,*DOB*	
City	City	No	*CITY*	([A-Z][a-z])+
Country	Country	No	*COUNTRY*	([A-Z][a-z])+

Figure 2 Metadata and data pattern driven data discovery

Transparent data collection

Enterprises should collect personally identifiable data through explicit notification and obtaining a clear and formal consent from the citizen.

Limit unwanted data access

Based on the usage of the data, access to the data should be limited and monitored. This ensures that data is accessed on a need-to-know basis only. Appropriate role based authentication and control solutions can be leveraged for the same.

Privacy-safe data processing

All data privacy policies defined by central data privacy governance committee should be digitized using various data protection controls such as data masking, tokenization or data encryption. All data requests should follow approval-based and automated workflow. These requests should be audited and notified to governing body. The automated workflow should validate the data requests against the consent and purpose before sharing the data. Real time consent management solution can be used to view the data at the moment. Data should be encrypted before transmitting data across network.

Wherever possible, organization should use fictitious data generation solutions for application development and maintenance activities. This further reduces the risk as it obviates the need to even access actual data for data protection purpose.

Organization's existing data processing framework should be enhanced for lawful data processing by building in house solutions or integrating with third party solutions.

Proactive privacy compliance

Enterprises should strive to incorporate privacy principles, to be at the very core of application design. Strategies such as data minimization, hiding, separation, etc. should be used to design the new applications. In addition, compliance of the existing applications can be achieved by profiling sensitive attributes and implementing remedial measures.

Data incident management and reporting

The data flow should be monitored and audited in automated way. The existing auditing framework should be enhanced to track usage of personal data. Any mismatch with enterprises' data policy should be notified to concerned authorities within defined SLA. The data privacy trends, scorecards and KPIs should be monitored regularly to validate the compliance.

Data retention

Enterprises should revisit data retention policy and take strategic decisions to destroy unwanted data, unless it needs to be stored as part of other regulatory requirements. The automated solution should be used to destroy or anonymize/encrypt the data periodically in accordance with the defined policy.

Conclusion

With enterprises across geographies and domains, now coming under specific data protection regulations, it is imperative for them to establish some formal privacy governance framework. This paper provides one potential approach for enterprises to create such a framework. This approach will enable enterprises to ensure need-based data access to external and internal stakeholders, process data in a privacy-safe way and create suitable controls around these activities.

REFERENCES

[1] Jayant Dani blog: http://sites.tcs.com/blogs/agile-business/gdpr-compliance-improves-data-governance/
[2] Jayant Dani blog : https://www.linkedin.com/pulse/internet-virtual-bounderies-jayant-dani/
[3] Jayant Dani blog : https://www.linkedin.com/pulse/privacy-attackers-jayant-dani/
[4] Website:http://ec.europa.eu/justice/data-protection/
[5] Website :https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost , subject to terms and conditions mentioned at https://itif.org/copyright
[6] Website : http://www.cbprs.org/
[7] Jayant Dani 2017. Article: Privacy_By_Design – Approach

Jayant Dani has over 20 years of industry experience. He is DSCI Certified Privacy Lead Assessor and Open Group Certified Master Architect. He played a leading role in setting up the Big Data practice at Tata Consultancy Services (TCS). Jayant Dani is currently spearheading the conceptualization, architecture, design, and engineering of TCS MasterCraft DataPlus, an integrated data management platform. His area of expertise includes technical leadership of large solution teams, client relationships, and management of large scale implementations. Jayant Dani is also passionate about architecting technology solutions across industry verticals and has many publications and patents to his credit.

Sameer Rane

Consultant

Sameer Rane has 14 years of IT industry experience. He played leading role in the maintenance, deployment and management of banking products operating in treasury and branch management space. His area of expertise includes technical leadership of solution delivery teams and customer relationships. Currently Sameer is presales consultant for TCS MasterCraft DataPlus, an integrated data management platform from TCS.