Building trust through effective data governance

August 2020

pwc

asg technologies®

Introduction

Data privacy is about providing individuals with the knowledge and ability to exercise discretion with respect to the types of data that is collected about them, where such data is collected from, the purpose of collection, and who the data is being shared with. This helps build trust by assuring stakeholders that an organisation's data management practices are efficient and safe.

Data privacy and related concerns on trust have emerged as global issues of importance. The world of data privacy has also shifted its focus from guidance to stepped-up enforcement. The large fines levied on some major multinational corporations (MNCs) by data protection authorities for non-compliance with data privacy regulations are making MNCs cognisant of the importance of data privacy.[1] Organisations are onboarding a significant number of resources to meet data-related requests from customers as they are increasingly exercising their rights over their own data. Catering to such requests requires multifaceted and holistic approaches involving business, legal, technology and information technology (IT) security leadership teams.

1. https://www.csoonline.com/article/3518370/the-biggest-ico-fines-for-data-protection-and-gdpr-breaches.html

01

The Personal Data Protection Bill, 2019[2]

In India, the Personal Data Protection (PDP) Bill, 2019, introduced significant changes to the Indian data protection regime. It is designed to strengthen and unify data protection by building data trust. The PDP Bill is expected to:

- protect the privacy of individuals relating to their personal data
- specify the flow and usage of personal data
- create a relationship of trust between persons and entities processing the personal data
- protect the rights of individuals whose personal data are processed
- create a framework for organisational and technical measures in processing of data
- create social media intermediary norms
- establish regulations for cross-border transfer and accountability of entities processing personal data
- propose remedies for unauthorised and harmful processing
- establish the Data Protection Authority (DPA) of India.

2. https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

02

Broad data governance attributes aligned to the PDP Bill's focus areas

Data discovery and traceability

- Classification of personally identifiable information (PII), sensitive personal information (SPI) and critical personal information (CPI)
- Periodic data audits

Data retention

- Polices and guidelines about retention of personal data

Data quality

- Completeness, accuracy and validity checks of personal data processed
- Periodic data audits

Data stewardship

- Security safeguards to avoid data breaches
- Transparency in the processing of personal data

Identity and access governance

- Role-based access to PII to enhance data security

Cross-border data strategy

- Guidelines for cross-border transfer of personal data

Source: PwC analysis of data from the Ministry of Electronics and Information Technology

Some of the key broad data governance categories that are aligned with the key focus areas of the PDP Bill, 2019, around data trust include:

- **Data discovery and traceability**

  Some of the key asks of the bill include identifying and updating PII, SPI and CPI data, and deleting data based on validity. Additionally, the bill mandates that organisations understand the flow of personal data across their systems and have a stringent data governance framework in place. The bill identifies record-keeping of entire data lifecycles and periodic data audits as other critical activities that organisations need to perform to be compliant.

- **Data retention**

  The bill provides guidelines on data retention, erasure and modification. Hence, it is the responsibility of the data fiduciary to ensure that methods of destruction, deletion or erasure of personal data are clearly stated and followed. A fiduciary is an entity or an individual with an obligation to act in a trustworthy manner in the interest of the data principal. A few examples of data fiduciaries include professionals like lawyers, doctors and directors of a company. Data deletion erases data but data is recoverable, while data destruction destroys the data permanently and the media.

- **Data quality**

  It has been mentioned that the data fiduciary shall take reasonable steps to ensure that personal data that is processed is complete, accurate, not misleading, updated and takes into consideration the purpose of processing. Accordingly, the data fiduciary should take reasonable steps to notify others or relevant entities of issues related to data quality. The data fiduciary should also have its policies and method of processing personal data audited annually by an independent data auditor. On basis of this practice, the data auditor may assign a rating in the form of a data trust score to the data fiduciary.

- **Data stewardship**

  The data fiduciary is responsible for defining and maintaining policies for processing of personal data. The policies also need to be audited annually by an independent data auditor. Accordingly, the data fiduciary should ensure that key areas such as processes adopted, transparency in data processing, security safeguards, personal data breach process flow and remediation are a part of the policy. This will help in data accountability, as mentioned in the bill.

- **Identity and access governance**

  Role-based authorised access to PII will help in data security, as required by the bill. The data principal (A) needs confirmation from the data fiduciary (B) whether B is processing or has processed A's personal data, as well as a brief summary of processing activities undertaken by B with respect to A's personal data. Appropriate action is to be taken by the data fiduciary or data processor in response to personal data breach. This will help in avoiding unauthorised access and processing of personal data. It will also help in tracking the origins of a breach in case of any such incident.

- **Cross-border data strategy**

  There should be clear information regarding any cross-border transfer of personal data that a data fiduciary intends to carry out. Transfer of personal data by a data fiduciary is subject to standard contractual clauses. Further, the fiduciary needs to certify and periodically report to the DPA that the transfer is made under a contract that adheres to such standard contractual clauses or intra-group schemes. Additionally, the fiduciary also needs to bear liability for the harm caused due to any non-compliance with the standard contractual clauses or intra-group schemes by the transferee.

03

Building customer trust through compliance with the PDP Bill

Building customer trust depends on the way an organisation manages its personal data. The journey to building customer trust requires organisations to establish a strong foundation and adequate data management processes.

Building customer trust in an organisation's data management practices has several components. Data discovery and traceability help organisations understand the movement of PII across the entire data lifecycle, thereby providing clarity and confidence. They help organisations to understand the process of deletion and modification of personal data, which can be helpful during data audits. Both of them help in identifying cross-border transfer of data, thereby ensuring that organisations are able to avoid non-compliance and penalties, as per the norms of the bill. Data quality norms help organisations understand the quality of data residing in the systems across the various data quality dimensions.[3] Policies defined by data protection officers (DPOs) and data fiduciaries as a part of the data stewardship requirement will help in standardising the processes for managing data. Access management will facilitate role-based authorised access to PII, thereby avoiding data breaches and unlawful access to personal data.

Some of the privacy challenges faced in building customer trust include locating and identifying PII, knowing how and why PII is being used, ensuring data transparency, securing personal data, using data ethically and managing new technologies for data management, thereby bringing about a cultural shift in the organisation.

3. Data quality dimensions include completeness, existence, integrity, consistency, accuracy, interpretability, uniqueness, availability and timeliness.

04

How PwC can help

PwC's Data Governance team has been continuously working in several data governance areas, including data privacy, to create a trust-based environment.

PwC's solution can help clients to:

- assess their compliance readiness with privacy regulations
- demonstrate accountability or re-engineer their privacy governance to show trust.

Some of the common data governance services offered by the PwC cover the following areas:

Strategy and council setup

- Privacy strategy and maturity assessment
- Privacy council and operating model
- Data ownership and accountability
- Standards, policy, process and control rules

Design and implementation data

- Discovery, inventory and classification
- Data traceability and lineage
- Data quality – profiling and remediation
- Data access and security
- Data architecture – consent, purpose and rights

Operational support

- Data trust and compliance dashboard
- Stewardship – programme and change management
- DPO-managed service support

Data life cycle governance

- Data acquisition
- Data processing
- Data sharing and transfer
- Data retention, archival and deletion

Source: PwC

A. Strategy and council setup

- Provide data privacy services, which include privacy assessment services for privacy maturity assessments and global privacy compliance assessment.
- Enable organisations to strategically govern their data and set up an operational data governance council.
- Drive the data ownership and accountability framework.
- Aid in understanding industry best practices, creating policies, processes, rules and templates.
- Implement and manage service support of data governance CoE.

B. Design and implementation

- Drive discovery, data flow discovery, transparency and traceability of data (e.g. generate automated reports to source traceability).
- Assist in development of a sustainable framework and key performance indicators (KPIs) to manage data quality.
- Drive data access and security of data and its sources, creating access entitlement matrix.
- Help with consent, purpose and rights management in the overall data architecture.

C. Data life cycle governance

- Accelerate data implementation programme prevent data swamp, assist with data migration governance, etc.
- Assist to understand and create data collection touchpoints inventory, and obtain consent for collection.
- Assist to understand data storage of sensitive personal information and its duration, rights and consent.
- Aid in understanding data processing regulations, compliance and process.
- Enable organisations to understand data sharing terms and conditions, privacy policies, cross-border transfer and data sharing technologies.
- Help draft data retenion, archival and deletion policies, including those related to process, duration, stakeholders and responsibilities.

D. Operational support

- Help build and transform the data trust of an organisation.
- Drive roles for stewardship, programme and change management.
- Assist organisations and data protection officer in ensuring compliance with privacy regulations.

05

ASG Technologies: Automating personal data classification and trust

ASG's Data Intelligence (ASG DI) and Mobius Content Services (Mobius) provide a unified platform for managing personal information. This unified platform allows current ASG customers to leverage their existing content management investment to locate personal data within structured and unstructured information and build a complete inventory of personal data – a critical foundation for compliance with privacy regulations. This approach helps in managing personal data more efficiently and reduces risks with a consolidated governance and compliance framework.

Main features

ASG DI is a powerful platform to provide a foundation for privacy management. It provides comprehensive automation capabilities for ingesting and understanding metadata from many sources and a business glossary providing semantic context. In addition, it enables identification and classification of PII, and offers a suite for the General Data Protection Regulation (GDPR) and privacy impact assessment (PIA) focused reports and dashboards, lineage of PII with optional flags, and PII cascading to automate PII identification to all downstream data elements in data lineage.

Mobius provides an open, flexible and scalable architecture to manage large volumes of information. It captures, governs and delivers digital content and assets generated by people, applications and machines at web-scale volumes and high-performance levels on demand. Content is managed throughout its lifecycle and is made available to people and processes, wherever and however needed.

Mobius provides policy-based, rule-driven governance services to precisely and securely manage and automate the lifecycle of enterprise content. Its role and user policies govern who can access, view and modify content. Content policies set rules to automatically capture, classify, encrypt, redact, retain and dispose of records.

This gives users the ability to comply with corporate governance and government regulations such as the GDPR, the California Consumer Privacy Act (CCPA) and others.

Who can use ASG's solutions?

Compliance and data privacy teams are the most common teams that can use ASG DI and Mobius platforms to gain a complete understanding of personal data and management of PIAs. Apart from these, governance staff can use the above-mentioned platforms to establish a unified foundation for structured and unstructured data governance and stewardship. Business analysts can use them to build trust and gain a faster and more detailed understanding of business processes and how data is used. Decision makers can use them to easily find, understand, trust and use structured and unstructured data.

06

Benefits of using ASG solutions

There are several benefits of using ASG's platforms. These include faster and more reliable GDPR and CCPA compliance, greater trust and understanding of personal data, accelerated detection of anomalies (e.g. fraud) through pattern recognition, reduced workload and improved collaboration.

Some of the other benefits include locating personal data within structured and unstructured information in the content services repository to build a complete inventory of PII, which is a critical foundation for compliance with privacy regulations. Also, structured and unstructured content metadata can be leveraged to build data catalogue data sets to train machine learning (ML) algorithms and support pattern recognition and analytical studies for:

- developing applications for fraud detection
- building a complete understanding of information supply chains by merging information from structured and unstructured sources to increase trust in data
- accelerating decision making by adding quality information and tagging personal data.

07

PwC and ASG – the combined value

The PwC-ASG combination offers distinct advantages to clients of all sizes, capabilities and across industries. Together, PwC and ASG help clients navigate and manage the new complexities of data privacy in the areas of technology, business impact, cultural shift, change management, regulatory requirements, response and governance. PwC and ASG help organisations across multiple industry segments build trust in data. In addition, they support clients in not only discovering and contextualising their data supply chain to more accurately understand how and where PII is proliferated throughout their IT landscape, but also building a disciplined process to achieve privacy compliance.

Case study

A leading private sector bank in India was looking to implement the data governance framework for its customer data.

The bank was also looking to set up the PII elements business glossary and end-to-end data lineage for those PII elements. Based on these business glossaries, the bank wanted to build access control matrix for PII elements.

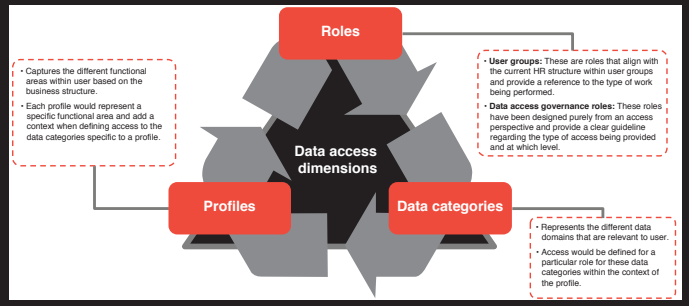
PwC and ASG helped the client:

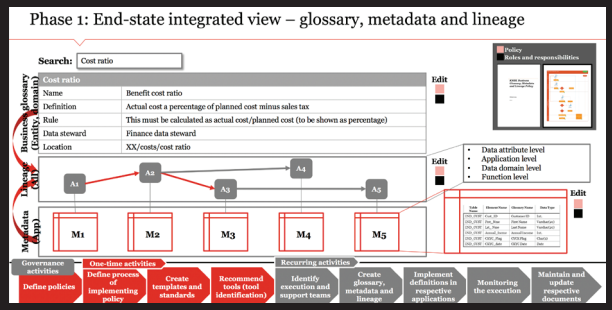
- to define the PII element business glossary, design approval and stewardship workflows
- prepare and publish the final policy for business glossary metadata, data lineage, change management and environment management
- implement end-to-end lineage for identified PII elements.

PwC utilised its Enterprise Data Governance Framework and ASG used its ASG DI product that helped the client drive the vision of governance for control and governance for growth.

Achievements

- Implemented PII elements business glossary.
- Created approval and stewardship workflows.
- Designed and implemented policies for business glossary, metadata, data lineage, change management and environment management.
- Implemented end-to-end data lineage for identified PII elements.
- Created data governance implementation approach and roadmap.





About ASG Technologies

ASG Technologies is an award-winning, industry-recognized and analyst-verified global software company providing the only integrated platform and flexible end-to-end solution for the information-powered enterprise. ASG's Information Management solutions capture, manage, govern and enable companies to understand and support all types of information assets (structured and unstructured) and stay compliant. ASG's IT Systems Management solutions ensure that the systems and infrastructure supporting that information lifecycle are always available and performing as expected. ASG has over 3,500 customers worldwide in top vertical markets including Financial Services, Healthcare, Insurance and Government. Visit us at ASG.com, LinkedIn, Twitter and Facebook.

Kaushik Bagchi

Vice President – Information Management Asia Pacific

kaushik.bagchi@asg.com

Mobile: +91 98672 65523

Vivek Vallathol

Director, Channels, ASG Technologies India

vivek.vallathol@asg.com

Mobile: +91 98404 59925

Suresh Sai Guru Prasad

Sales Manager, ASG Technologies India

suresh.guruprasad@asg.com

Mobile: +91 96198 64527

Erwin J. Anderson-Smith

Global Alliance Director, ASG Technologies, Inc

erwin.anderson-smith@asg.com

Mobile: +1 602 284 2842

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in advisory, assurance and tax services. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details. For more information about PwC India visit us at www.pwc.in

Contact us

Sudipta Ghosh
Partner and Leader, Data Analytics Technology Consulting
PwC India
Mobile: +91 99874 34327
sudipta.ghosh@pwc.com

Mukesh Deshpande
Partner and Leader, Data Management and Governance Lead Technology Consulting
PwC India
Mobile: +91 98450 95391
mukesh.deshpande@pwc.com

Amit Lundia
Director and Leader, Data Governance Technology Consulting
PwC India
Mobile: +91 98369 22881
amit.lundia@pwc.com

Saurabh Pramanick
Manager, Data Governance Technology Consulting
PwC India
Mobile: +91 99679 18427
saurabh.pramanick@pwc.com

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2020 PricewaterhouseCoopers Private Limited. All rights reserved.

KS/August 2020-M&C 7037