VIEW POINT

PRIVACY FIRST DATA DISPOSAL FOR PERSONAL DATA PROTECTION THROUGH COHESITY

Abstract

Many enterprises struggle to manage the personal data of their customers, employees, and partners. They remain overwhelmed by the sheer volume and variety of the data at their enterprise.

Most organizations let lawyers and compliance teams design their storage policies. Setting limits to storage with a clear policy on retention periods and secure data disposal is needed for data privacy. Enterprises need help in demystifying storage limitations and understand the impact of customer trust, storage cost, and your organization's compliance with the key regulations.

This whitepaper aims to set a framework and provide insight on the best-of-breed Privacy Platform from Cohesity and Infosys. Our proposition for a privacy-first data life cycle includes end-of-life disposal for better data utility while managing personal data protection.

COHESITY

Infosys®
Navigate your next

Table of Contents

1. The domino effect of Data Storage Limitation and impact on Privacy..... 3
2. Key Challenges faced by Organization Data retention and destruction..... 3
3. Quantifying the Impact of Storage Limitation – An Enterprise Use case in the Auto Sector..... 4
4. Infosys PrivacyNext Platform Powered by Cohesity..... 5

The domino effect of Data Storage Limitation and impact on Privacy

Organizations collect large volumes of data on their customers, partners, and employees. This data is beneficial to improve business outcomes. For instance, analysis of employee data gives insights on the risk of an employee leaving the organization to competition. The same information can pose a substantial data privacy risk to the employee.

The business should always review the personal data it stores about an employee and only preserves enough data to deal with. The company should permanently delete the information that is not required at certain intervals of time. Ensuring proper erasure of data will reduce the risk of keeping irrelevant, inaccurate data.

Further, there is a need for robust data deletion for data minimization and accuracy for compliance and optimizing storage costs for organizations.

This whitepaper focuses on advocating the right balance of retaining valid data and minimize storage by deleting the information which is not relevant or is a potential privacy breach for the organization. We recommend a comprehensive risk-driven approach to dispose of Personally Identifiable Information (PII) through:

- Complete Data Discovery to identify sensitive information in the ecosystem
- Building a Data Disposal Policy taking into consideration the compliance and regulation need of the organization
- Implement best of breed privacy technology platforms for managing data and optimizing storage cost

Key Challenges faced by Organization Data retention and destruction

Personal data is susceptible to unauthorized access and use, so keeping it beyond its useful life risks the organization. Moreover, there is no major compliance with an organization's excessive data retention practices unless discovered following a security breach.

HIPAA | Sarbanes-Oxley Act | GDPR | OSHA | CCPA | PDPA | Privacy Law | IT Bill | PDPA | DPA | DPL | Privacy Act | Privacy Act | PPA | POPI

1. Data Collection
2. Use and Purpose
3. Data Subject Rights Mgmt.
4. Storage Limitation
5. Transparency
6. Data Accuracy
7. Data Transfer

The challenges can be classified across different key categories as per European Union's General Data Law Regulation:

1. Data Collection – Organizations struggle to collect data from multiple data sources without a purpose or well define retention policy. Privacy is always an after-thought in the collection and ingestion process.
2. Use and Purpose – Organization also struggle to justify the use of data for legitimate, specific, and explicit purpose only and not for incompatible purposes
3. Data Subject Rights Management - Provide rights to Data Subjects to access, modify and know information about their data. This adds an overhead to the governing enterprise to manage

and ensure the Data subjects are communicated on the data used.

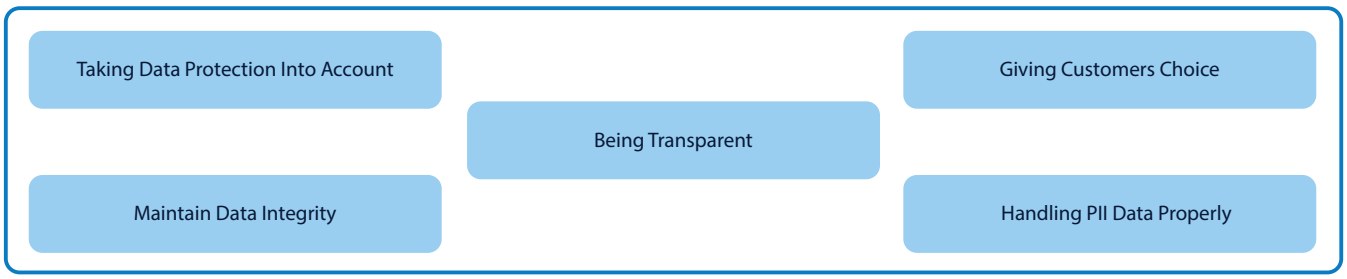
4. Storage Limitation - Many businesses keep adding racks into their data centers as their data store keeps growing with time, so physical space limitation is always a persistent problem. Storage limitation is a crucial challenge faced by organizations across the globe.
5. Transparency – As per the new federal court rules, organizations should pay more attention to how their business process stores the data and dispose of business-related documents in case of litigation. There is a need to manage the end user's consent and ensure complete data transparency even during data disposal.
6. Data Accuracy – One critical need to accelerate data disposal is the need to ensure the data accuracy to be maintained across multiple data sources.
7. Data Transfer – There is a need to ensure the data is managed across the organization's boundaries and securely transferred outside or within multiple GEOs considering cross-border transfers. There are gigabytes of data that is transmitted without compliance checks or cross-border flows.

Quantifying the Impact of Storage Limitation – An Enterprise Use case in the Auto Sector

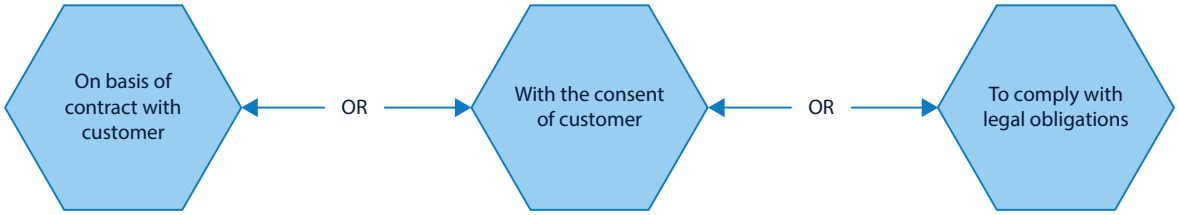
Organizations that have failed to routinely purge personal data that is no longer being processed for its original purpose will struggle mightily to meet the GDPR - Article 5 retention restrictions. Various automobile manufactures have faced and still face multiple hurdles, especially in implementing data protection law in the development of multiple technologies

How Information is gathered for Automotive Makers:

Manufactures commit to:



Case when Automobile Manufactures share PII Data:



There are three key categories of data protection that are needed for Auto manufactures:

Business Function	Data Privacy Controls
Automotive aftersales	Data protection in a regulation compliant organization for all the data flow in automotive aftersales process, which includes the transfer of customer data among various stake holders like dealers, manufacturers and distributors
Product Development and Manufacturing	Organization collect various types of data, including sensor information and camera images of Traffic routes, situations and road signs, weather conditions to efficiently manage their large operation chains.
Connected Vehicle Experience	The continuous improvement in technologies in space of AI/ML is steadily generating and increasing the large amounts of data. This data is needed for controlling various vehicle functioning. Other data is transmitted to the externally located vehicle functioning to provide functionalities and services.

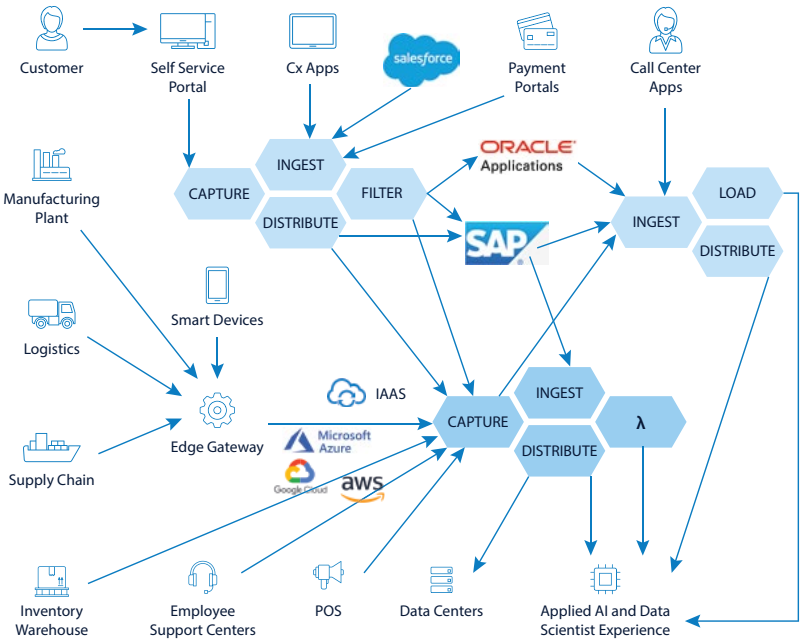
Infosys PrivacyNext Platform Powered by Cohesity

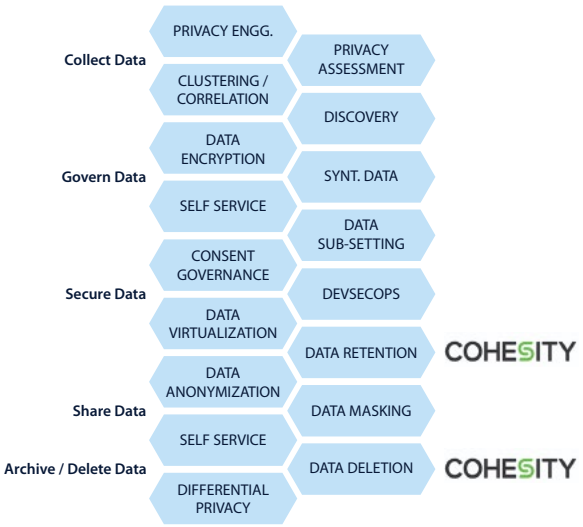
Strict data retention policies and practices are not only required for regulation but are also crucial in risk mitigation for any data-driven enterprise. Sensitive data must be deleted, destroyed, and anonymized and should no longer be vulnerable to breach. Furthermore, robust data destruction and end of PII disposal enables the organization to adopt a Privacy First approach in dealing with data.

Through the Infosys Innovation Network (IIN), a well-orchestrated partnership between select startups and Infosys to provide innovative services to our clients, we integrate startups into broader Infosys platforms and de-risk their implementation for clients. Infosys PrivacyNext Platform powered by IIN partner Cohesity offers an intelligent Privacy First Fabric for your organization.

This collaborative offering ensures that your data is governed and disposed of/ protected promptly. The Privacy Platform focusses on:

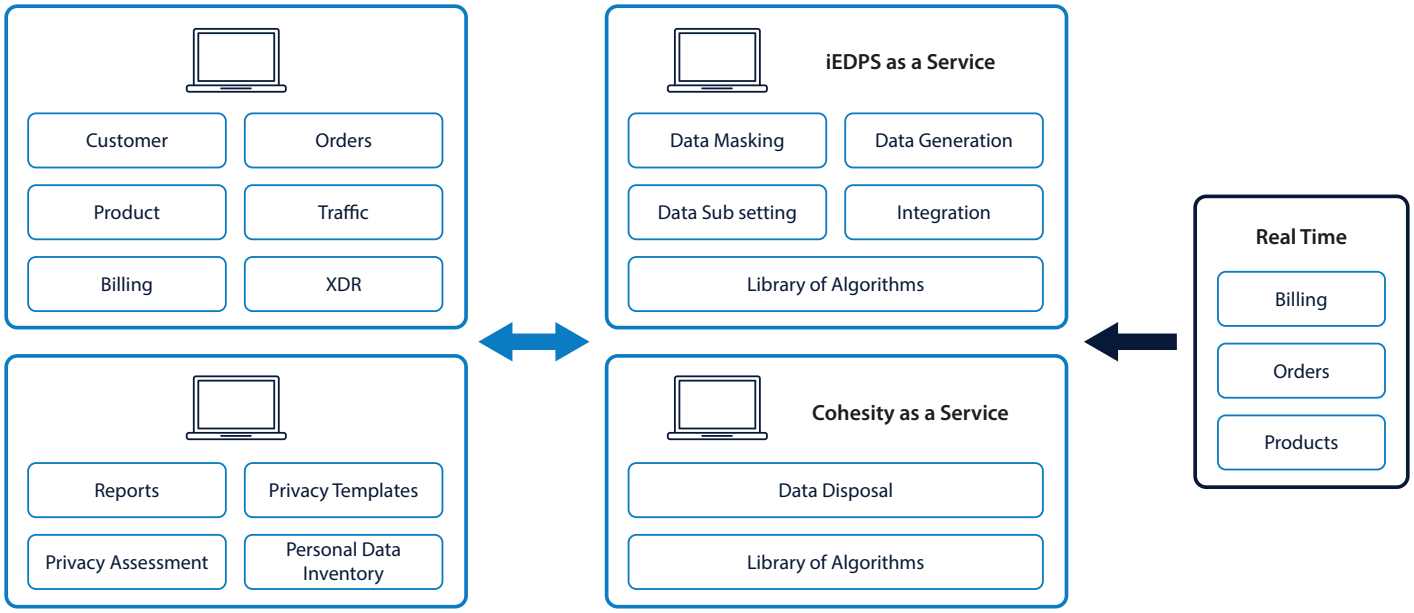
1. Zero Trust Model and Identity Management – Built-in security standards to discover, capture, and protect biometric authentication from users, including data on fingerprints, photos, videos, voice, physiological recognition, and DNA signatures.
2. Service-Oriented Security – Flexible architecture for integration with multiple data stores. The platform focuses on improving the current encryption standards, including reinforcement with Quantum encryption standards.
3. Privacy and Security Assessments – 5G needs an open software and hardware ecosystem to be audited and assessed regularly to comply with emerging regulatory norms.
4. Rigorous user privacy protection and consent governance – The platform helps avoid any data leak without proper consent governance.
5. Data Archival Services – Data deletion and archival services on data, including edge sources.
6. Data Augmentation for ML – There will be petabytes of data shared for AI/ML algorithm learning and training. The platform also provides synthetic data generation or anonymization of data sets.





Cohesity provides unique capabilities to manage data copies for various testing, reporting, DR, archival, and more that help generate value by running custom applications natively on the platform. One can communicate with the repository securely via APIs. Some of the capabilities that can be leveraged include:

- Provisioning zero cost clones that can be scrubbed to identify the PI data that can be masked
- Identify PII on unstructured data through pattern matching by regular expressions
- Data lock and legal hold
- ML-based reporting on anomalies
- Ability to verify the VM images against CVE
- Support unlimited scalability, global de-dupe to provide lasting efficiency



Infosys PrivacyNext aims to build a Privacy First Organization leveraging global talent, strategic partnerships, and best in class privacy-enhancing technologies to minimize data risk.

The platform is powered by Infosys Enterprise Data Privacy Suite (iEDPS). iEDPS provides enterprise-class data privacy capabilities and enables an organization to adhere to global regulatory standards such as GDPR, CCPA, HIPAA, PIPEDA, GLBA, ITAR, other global and local regulations.

Loaded with deterministic, selective, dynamic, and static masking features, Data Discovery, and Data Generation capabilities, iEDPS can be deployed on any platform and supports all major databases and file systems.

About Us

The incubation center of Infosys called 'Infosys Center for Emerging Technology Solutions' (iCETS) focuses on the incubation of NextGen services and offerings by identifying and building technology capabilities to accelerate innovation. The current areas of incubation include AI & ML, Blockchain, Computer Vision, Conversational interfaces, AR-VR, Deep Learning, Advanced Analytics using video, speech, text, and much more.

To know more, please reach out to iCETS@infosys.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next