ENTERPRISE DATA PROTECTION WITH INFOSYS ENTERPRISE DATA PRIVACY SUITE

Infosys®
Navigate your next

Organizations today need to focus on customer privacy in a data regulations driven industry. With the large volume of data that is spread across a multi-dimensional data landscape, securing, and protecting an organization's data is highly imperative and critical. Organizations now are investing in Data Privacy for the following reasons:

- Sensitive information is getting hacked and leaked more than ever and organizations are at risk of getting burned

- Growing data privacy regulations are increasing cost of privacy compliance, monitoring protection and management

- Changing workforce dynamics and boundary-less customer and IT services requires ubiquitous data access

- With millions of employees working from home, organizations must focus on building a secure, new-age digital workplace to support remote working.

Along with increasing demand for data privacy, managing test data using traditional Test Data Management (TDM) practices is also getting challenging due to its inability to accelerate cloud adoption, protect consumer data, provide reliable data, ensure data consistency, and automate and provision test data. Organizations need an alternative to the traditional approach of sub-setting, masking and reserving production data for key business analytics and testing.

The Infosys Solution

Infosys Enterprise Data Privacy Suite (IEDPS) is a patented, enterprise-class data security suite which enables organizations to protect and de-risk sensitive data. It helps organizations reduce the cost of compliance. IEDPS is a one-stop solution for protection of confidential, sensitive, private, and personally identifiable information within enterprise repositories.

Infosys Privacy First Value Chain

Find your Data	Secure your Data	Share your Data	Monetize, Audit and Delete Data

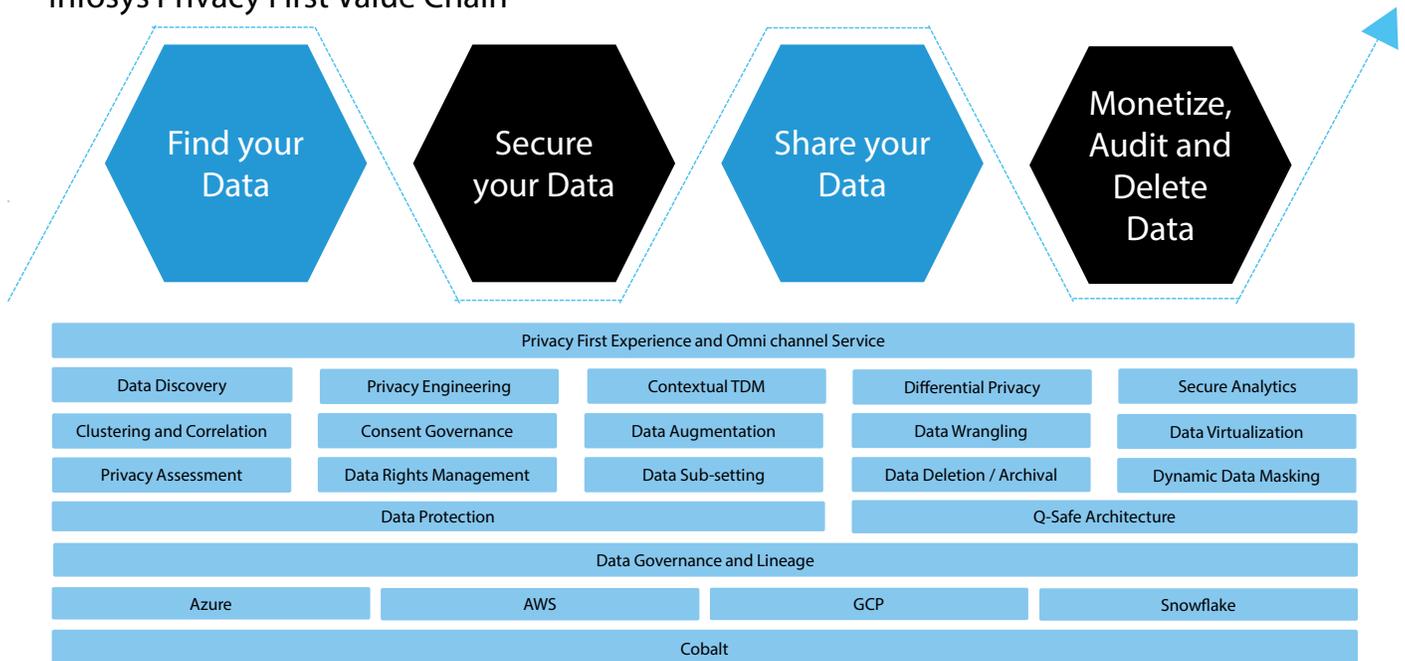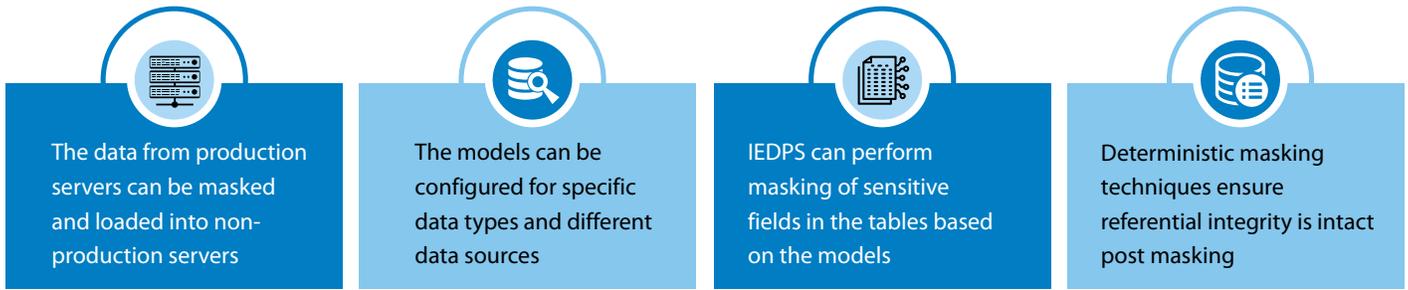| Privacy First Experience and Omni channel Service				
Data Discovery	Privacy Engineering	Contextual TDM	Differential Privacy	Secure Analytics
Clustering and Correlation	Consent Governance	Data Augmentation	Data Wrangling	Data Virtualization
Privacy Assessment	Data Rights Management	Data Sub-setting	Data Deletion / Archival	Dynamic Data Masking
Data Protection			Q-Safe Architecture	
Data Governance and Lineage				
Azure	AWS	GCP	Snowflake	
Cobalt				

Figure 1 – Infosys Privacy First Value Chain

Sensitive data discovery

Data discovery module identifies sensitive PII data, using regular expressions and key-words semantic matching across a diverse set of data sources. IEDPS provides sensitive data discovery through the following capabilities:

- Set pre-built templates based on data protection act

- Provide matching on data pattern, metadata

- Connect to diverse set of data sources
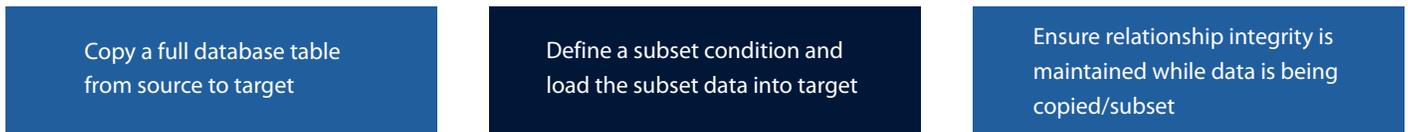
- Ability for the teams to export to excel, PDF

Data masking

IEDPS provides 180+ obfuscation algorithms that can be used to anonymize the data from non-production servers. It intelligently loads obfuscation rules applicable to the type of data.

The data from production servers can be masked and loaded into non-production servers	The models can be configured for specific data types and different data sources	IEDPS can perform masking of sensitive fields in the tables based on the models	Deterministic masking techniques ensure referential integrity is intact post masking

Data sub-setting

IEDPS is used to

Copy a full database table from source to target	Define a subset condition and load the subset data into target	Ensure relationship integrity is maintained while data is being copied/subset

Next-Gen test data management

IEDPS provides test data management and generates synthetic data for testing and analytics with more than 70 algorithms.

- Provides one-click data generation for all tables in hierarchy

- Generates contextual test data for accelerating development and testing for data driven products and services

- **Data refresh -** IEDPS provisions test environments with consistent sets of

masked production data topped up with synthetically generated test data

- **Workflow based TDM processes** – Defines data provisioning workflows to streamline process

- **Data augmentation** – Generates real like data for multiple scenarios in any desired volume. Leverages generated

data to train AI-ML programs enabling accurate predictions.

- **Data lake protection** – Provisions test environments on data lake for AI/ML

- Has AI-based self-learning algorithms for analytics data sets

- Has ability to create data in different formats

Types of data that can be generated

Data protection

Generalization

Perturbing data

Differential privacy & resistance to reconstruction

Structured data
Provide structured data for analytics

Pre-set files
Data generation of files

Unstructured data
Logs and chat transcripts

Images
Provide images for UX testing / AR-VR Kits
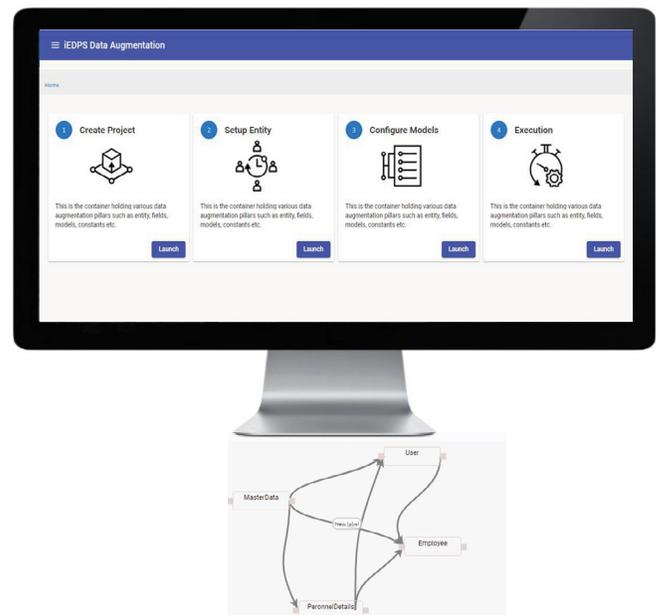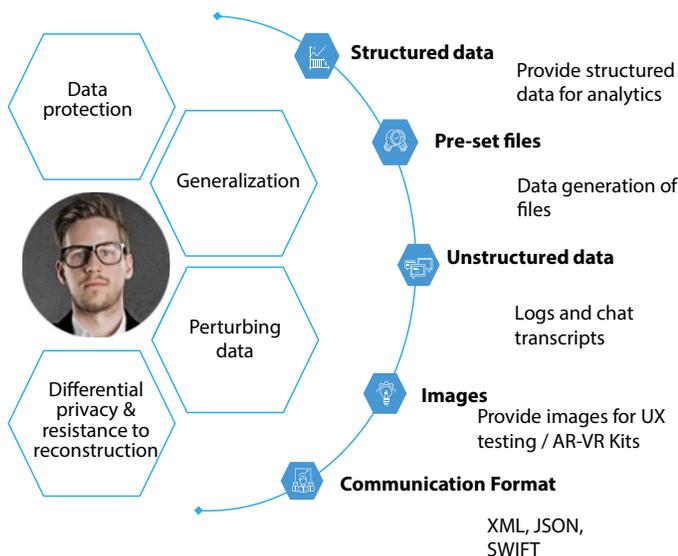
Communication Format
XML, JSON, SWIFT

Figure 2- Contextual Test Data - Different formats of Test Data

Data virtualization

IEDPS supports dynamic data masking for data anonymization and pseudonymization of critical production data through a virtualized data layer.

It creates a logical data layer on top of production database	Logical data layer/virtual database is used to query from a querying tool or any other application

On-demand obfuscation services

On-demand module of IEDPS

Provides a masking service that would be deployed at client-end	The application/web services are changed to invoke this IEDPS service whenever it deals with any sensitive information based on user role

Benefits

- IEDPS can effectively scale up to masking millions of records
- Supports wide range of data sources
- Ensures availability of high-quality test data thereby improving quality of testing

- Can be deployed to automate data masking, thus achieving up to 40% productivity improvement
- Successful implementation experience across various regulations such as EU GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), CCPA (California Consumer Privacy Act), PCI DSS (Payment Card Industry Data Security Standard) and others
- Varied platform support and multiple modes of deployment (on-premise and hosted)

Why Choose Infosys

Infosys helps enterprises create and execute strategies in their privacy transformation. We help our clients focus on the right areas to solve, and to solve these effectively. Our team of privacy experts, across the globe, is differentiated by the imagination, knowledge, and experience, across industries and technologies that we bring to every project we undertake.

Infosys has one of the largest TDM practices in the industry. With 100+ TDM engagements, 30+ tools alliances, 50+ IPs and 100+ accelerators, we believe that we are in a unique position to participate in the strategic journey enterprises are taking to build a secure Test Data Management service. TDM as a specialized services practice group at Infosys, has constructed the framework, to build test data capabilities consisting of underlying foundation of Tools-Process-People and service catalogue tailored as per client needs.

Success Stories

- **40% productivity improvement for a leading American bank:** Streamlined data provisioning process, helped set-up a centralized data privacy COE to ensure that various project teams comply to data privacy policies and all sensitive data in organization across various LOBs is consistently masked for usage in non-production environments (both onshore and offshore).

- **40% reduction in effort for a multinational investment bank** based in Europe. IEDPS was used to mask databases on refresh non-production environments. Enabled faster time to market with ability to scale up the resources needed for testing as required at offshore. Powerbroker based access control was devised, which enabled offshore access only to the masked environment.

Infosys®
Navigate your next

For more information, contact askus@infosys.com

Infosys.com | NYSE: INFY

Stay Connected