Wipro’s Data Privacy Solution

Powered by Microsoft Priva

wipro | CyberSecurity by CyberSecurists.

Wipro Data Privacy Capability

25+ Years of experience

100+ Customers for Data Privacy

300+ Privacy Professionals Globally

360º Partnership with Data Privacy Vendors

150+ Certified Privacy Professionals Globally

Phase	Assess	Analyze	Design	Rollout	Sustain
Services	• CCPA / GDPR / LGPD Readiness Assessment & roadmap definition • Privacy Impact Assessments • Vendor Privacy Assessments • Cloud Privacy Risk Assessments • Breach Response Assessment	• Policy & Control Gap Analysis • Privacy Threat Modelling • Data Classification • Data Discovery	• Privacy Framework Development • Privacy by Design • Privacy Engineering • Consent Management • Cookie Consent Management	• Data Anonymization • Data Encryption • Tokenization • Subject Access Request Automation • Recovery Plans • Breach Notification Automation	• Privacy Audits • Privacy Control Testing • Privacy Controls Assurance

Data privacy - From backroom to boardroom

Top 3 reasons for data breaches

- Malicious code
- Employee negligence
- Criminal attacks

$445 Bn

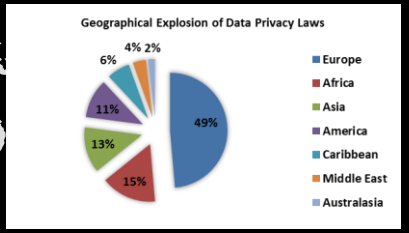
Is the annual cost of data breaches to Global economy

4%

Of Annual worldwide turnover is the fine for non - compliance with GDPR

$ 3.8 Mn

Is the average cost of data breach for organizations around the world



Impact of data breaches

- **Regulatory Fines**
- **Loss of customer trust**
- **Loss of reputation**
- **Loss of brand equity**

Data privacy – from backroom to boardroom

Data breaches are making headlines worldwide and hence data privacy have become a focal point for regulations and for discussions in boardroom.

Are organizations ready to adapt requirements of applicable privacy laws like GDPR, CCPA, PIPL?

Privacy by Design, Privacy by Default & Right to be Forgotten

4% of global turnover as fines for non-compliance

Mandatory Breach Notification

Consumer awareness

Consumers want Transparency, Notice & Choice in exchange for Trust

Contextual Privacy

Adopting a contextual approach to privacy can help build brand differentiation for organizations.

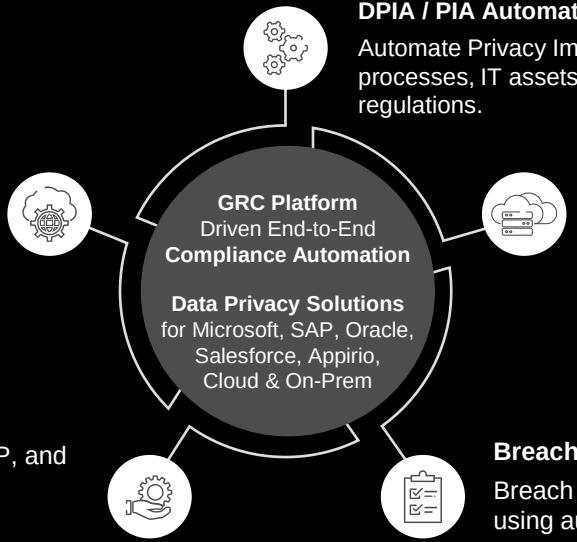
Solutions to accelerate your data privacy journey…

Privacy by Design

Automation & Analytics Powered by AI

Security by Design

Wipro's Data Privacy Solutions



DPIA / PIA Automation

Automate Privacy Impact Assessments for the applications, business processes, IT assets & new business initiatives impacted by privacy regulations.

Data Privacy Inventory

Single Source of Truth for personal data processing

Data Protection

Comprehensive lifecycle management of protecting data in enterprise, cloud using controls such as discovery, anonymization, encryption etc.

Individual Rights Management

Automate Individual Rights Management across ERP, and other enterprise systems using orchestration and automation engine.

Breach Notification & Reporting

Breach Notification & Reporting for 40+ data privacy acts using automated playbooks

Data Privacy Challenges

Key Data Privacy challenges

01 Data Governance Complexity due to acceleration of digitalization

02 Increased data breaches across industries globally

03 Lack of knowledge of personal data in the enterprise

04 Adoption of new horizon technologies

05 Lack of data privacy talent as the demand exceeds the supply

What We Hear in the Industry?

How Do I Make Sure –

- How to gain new insights from data and make better decisions, and to do so in a manner that protects individual privacy?
- How to provide individuals with new ways to exercise choice and control, especially where data uses most affect them?
- How to implement controls based on criticality of risk when there is lack of guidance from regulators?
- How to notify individuals when data is passively collected from machine to machine transactions?
- How do we ensure that there is no “bias” in decision making when processing personal data using AI & ML technologies?

Data Privacy Challenges Affecting 3E's

Experience

- Lack of knowledge/awareness of personal data in the enterprise; no single source of truth for personal data processing.
- Adoption of technologies like IoT, Blockchain, cloud, mobility poses new privacy risks
- Manual processes to manage data privacy requirements
- Inability to apply data privacy controls in fragmented and legacy systems

Efficiency

- Administrative activities in data privacy operations use up valuable time from the skilled privacy professional's daily schedule
- Lack of visibility into stakeholder functions (Business, IT, Compliance, Legal etc.) means silo'd operations and lack of process coverage
- Time consuming manual support for the business functions
- Inability to integrate privacy risk into overall enterprise risk and report your risk posture

Economics

- Limited scale of data privacy resources leads to inability to serve business; Adding resources results in increase in program cost
- Lack of objective and timely insights mean delayed decisions and elongated budgets.
- Support model with multiple dedicated teams mean an in-efficient and un-economic allocation of resources.
- Constraints in budget allocation result in data privacy solution being half-baked and ill-suited for purpose.

Data breaches are real and they result in loss of trust with your end customers. In this age of privacy, 'Trust' will be the factor that decides whether a business thrives or goes extinct, not 'service', or 'loyalty', or 'reputation'.

Our Guiding Principles and Approach

Our Solution Themes for Data Privacy

Experience

Consistency

- Standardized data privacy process and standards to cater to the needs of organization across various business units and functions

Flexibility

- Ability of the solution to dynamically adjust to the global data privacy requirements and compliance initiatives

Ease of Use

- Ability to Privacy by Design into the new products and services through a repeatable and sustainable process.

Efficiency

Intelligent Automation

- Using AI/ML capabilities in the data privacy operations means the efforts of the skilled privacy professionals are optimally utilized

A Common Risk language

- A uniform framework and standardized testing methodology means the ability to align with enterprise privacy management methodology

Integrated Processes

- Integrate the requirements of various stakeholders into the privacy management platform to ensure adequate and timely participation in decision making

Economics

Accelerate Decision making

- Objective insights from privacy impact assessments and control monitoring feeds mean that management can take risk-informed decisions

Scalability

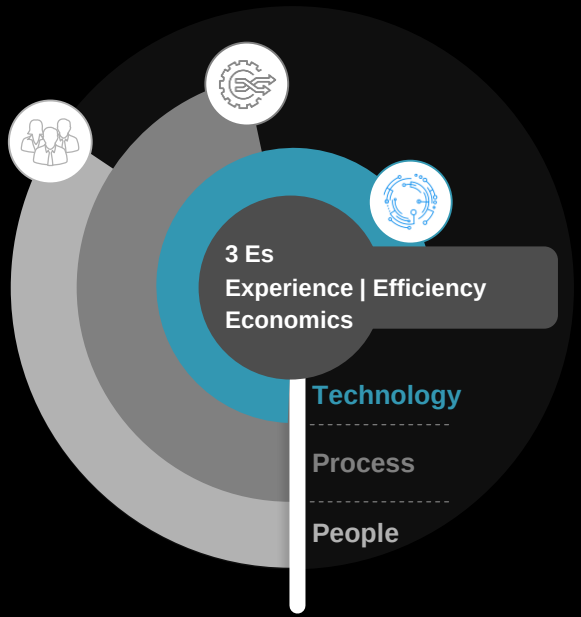
- Build a process and data privacy platform that is easily scalable and can be leveraged to comply with ever evolving data privacy regulations

On-Tap Support

- A flexible support model means dynamic allocation of resources to support your varying workloads and requirements

Our solution themes enables organizations to leverage privacy as a brand differentiator

Our Guiding Principles



- Assess
- Analyze
- Design
- Rollout
- Sustain

- Comprehensive Data Privacy Framework
- Integrated Workflow Automation
- Seamless External Integrations
- Intuitive Artificial Intelligence

- Data Privacy Framework
- Maturity Assessment
- Privacy by Design
- Data Privacy Threat Modelling
- Data Discovery
- Data Subject Access Requests
- Breach Notification
- Consent Management
- Cookie Compliance
- Privacy Impact Assessment
- Privacy Control Testing
- Subject Access Request Automation
- Vendor Privacy Assessments

We enable organizations to build and sustain a scalable data privacy program through a robust privacy framework

Wipro's Privacy Framework

Controller

Discover	Manage	Protect	Record	Report
Data Classification	Data Protection Impact Assessments (DPIA)/PIA	Encryption Management	Controls Assurance	Documentation
Data Discovery	Consent and Choice	3rd Party Risk Management	Audits	Certification
Data Mapping & Data Inventory	Individual Rights Management	Security Controls	Breach Management	Code of Conduct

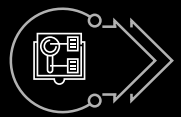
Privacy Principles				
Fair & Lawful Processing	Purpose Specification	Data Minimization	Choice & Consent	Data Quality
Transparency & Openness	Data Security	Data Access	Responsible Data Sharing	Accountability

Program Management, Compliance, Privacy & Security by Design, Governance & Risk Management

Privacy Metrics & Key Indicators

Technology, Automation & Reporting

Processor



Our Data Privacy Framework allows organizations to design & implement a forward looking privacy program that will enable compliance to ever evolving privacy regulations.

Wipro's Approach

Assess

Maturity Assessment of current data privacy program across people, process and technology dimensions and benchmarking against best practices and industry peers. Development of strategic roadmap for maturity enhancement.

Key Deliverables:

- Readiness / Maturity Assessment for Data Privacy
- Gap Analysis Report
- Program Uplift Recommendations
- Maturity Benchmark with Industry Peers
- Strategy including Operating Model and Execution Roadmap
- Stakeholder RACI Document

Key Outcomes:

- Identification of improvement areas with steps for remediation
- Defined target maturity level phased implementation plan to get there
- Revised governance model for alignment across stakeholders

Transform

Transformation of current data privacy program across people, process and technology dimensions based on outputs of assess phase to improve experience, efficiency and economics of operations and raise maturity of the privacy program.

Key Deliverables:

- Data Mapping and Data Inventory to create a "Single Source of Truth" for Personal Data processing.
- Enhance and implement scalable Data Privacy Policies & Process for Data Subject Access Requests fulfillment and Privacy Impact Assessment, Privacy by Design requests, Breach Notification.
- Consent lifecycle management & data privacy controls such as anonymization, data encryption etc.

Key Outcomes:

- Single Source of Truth for Personal Data Processing
- Knowledge of data flow throughout the data lifecycle
- Privacy and Security by Design and by Default
- Greater risk visibility

Sustain

Support ongoing operations of data privacy program, including maintenance and upkeep of technology solution and execution of end-to-end data privacy operations activities.

Key Deliverables:

- Privacy Impact Assessments for applications & business processes
- Privacy audits and data privacy control testing
- Privacy awareness through gamification and online campaigns
- Data Subject Access Requests fulfillment
- Privacy by Design guidance to business stakeholders

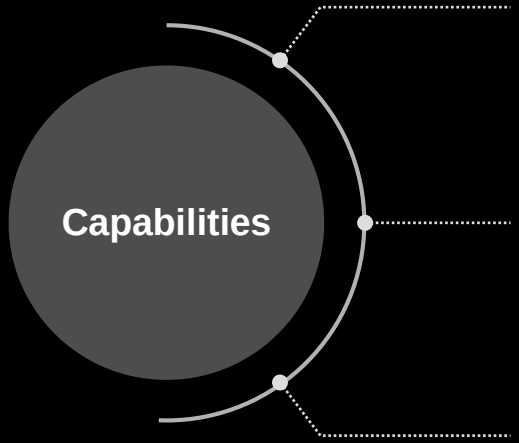
Key Outcomes:

- Privacy aware culture
- Data Privacy automation through automation and analytics powered by AI
- Cost optimized global support model

Microsoft Priva - Privacy Risk Mgmt Solution

Microsoft Priva - Introduction

Microsoft Privacy Risk Management solution that provides visibility into your organization's M365 privacy data and reduce risks through policies; Priva Subject Rights Requests feature provides automation and workflow tools for fulfilling data requests at scale.



- Identify critical privacy risks and conflicts
- Automate privacy operations and response to subject rights requests
- Empower employees to make smart data handling decisions

Microsoft Priva - Privacy Management solution for Microsoft 365

Organizations can see privacy related data status with volume, category, location, and movement of personal data in their Microsoft 365 environments. Additionally, they get visibility into the current status and trends of the associated privacy risks arising from personal data being overshared, transferred, or unused.

- **Identify critical privacy risks and conflicts**
- **Automate privacy operations and respond to subject rights requests**
- **Empower employees to make smart data handling decisions**
- **Automated Discovery**
- **AI-based Privacy Management**

Location for Microsoft Privacy management

- Exchange Online
- SharePoint Online
- OneDrive for Business
- Microsoft Teams

Microsoft Priva - Features

Automated Discovery

Privacy Management for Microsoft 365 **uses artificial intelligence** to assess privacy risks. It also has an automated discovery process whereby sensitive data get located.

AI-based Privacy Management

AI-based privacy management solution for Microsoft 365, which applies intelligence to quickly assess your organization's privacy risks and help anyone working with personal data make the right decisions.

Identify and protect against privacy risks

Proactively identify and protect against privacy risks such as data hoarding, data transfers, and data oversharing

Manage subject rights requests

Enable users to effectively manage data and take steps to comply with evolving privacy regulations Manage subject rights requests at scale

Find and visualize personal data

- Privacy management helps organizations to discover personal data automatically and provide key analytics and insights to admins to help them understand the privacy issues and associated risks in their organization. These insights are presented within your **Overview** dashboard, which provides automatic updates about your data with important trends, and the **data profile**, which allows you to explore ongoing analytics.
- **Gain visibility into the storage and movement of personal data**

Efficiently fulfill personal data requests

Privacy management provides you with the capability to automate **data subject rights** fulfillment with easy access to relevant data and customizable workflows that fit into existing business processes.

Integrate with Compliance Manager

Compliance Manager offers data protection and privacy assessment templates that correspond to compliance regulations and industry standards around the world. Taking steps in privacy management to protect the personal data you store can contribute to your privacy assessments in Compliance Manager and can help improve your compliance score.

Manage privacy risks at scale

Privacy management provides tools to detect these risks, establish policies and processes for remediation, and directly notify your users about issues and recommended actions to take.

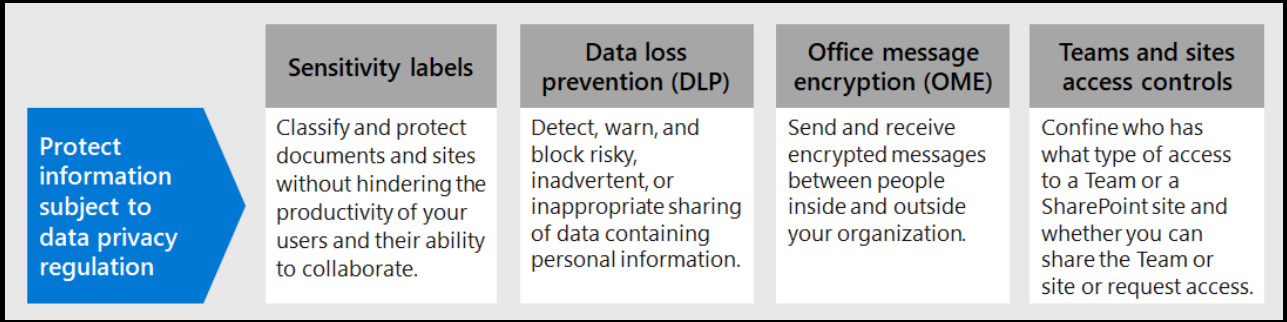
Built-in, customizable templates

Privacy management provides built-in, customizable templates for establishing ongoing policies tailored to these scenarios:

- **Overexposed personal data**: Discover open and over-privileged personal data in your organization and prioritize remediation efforts to secure data. Easily manage access rights to this data to protect privacy and prevent inappropriate use.
- **Data transfers**: Detect and manage transference of personal data between departments in your organization or across country or regional borders. This can help reduce the risk of data exposure, or of stepping out of accordance with privacy regulations and laws.
- **Data minimization**: Identify personal data that does not need to be retained and prioritize remediation efforts to delete this data.

Once set up, you can evaluate your data on an ongoing basis, receive alerts when policy matches are detected, and set up email notifications

Protect information subject to data privacy regulation



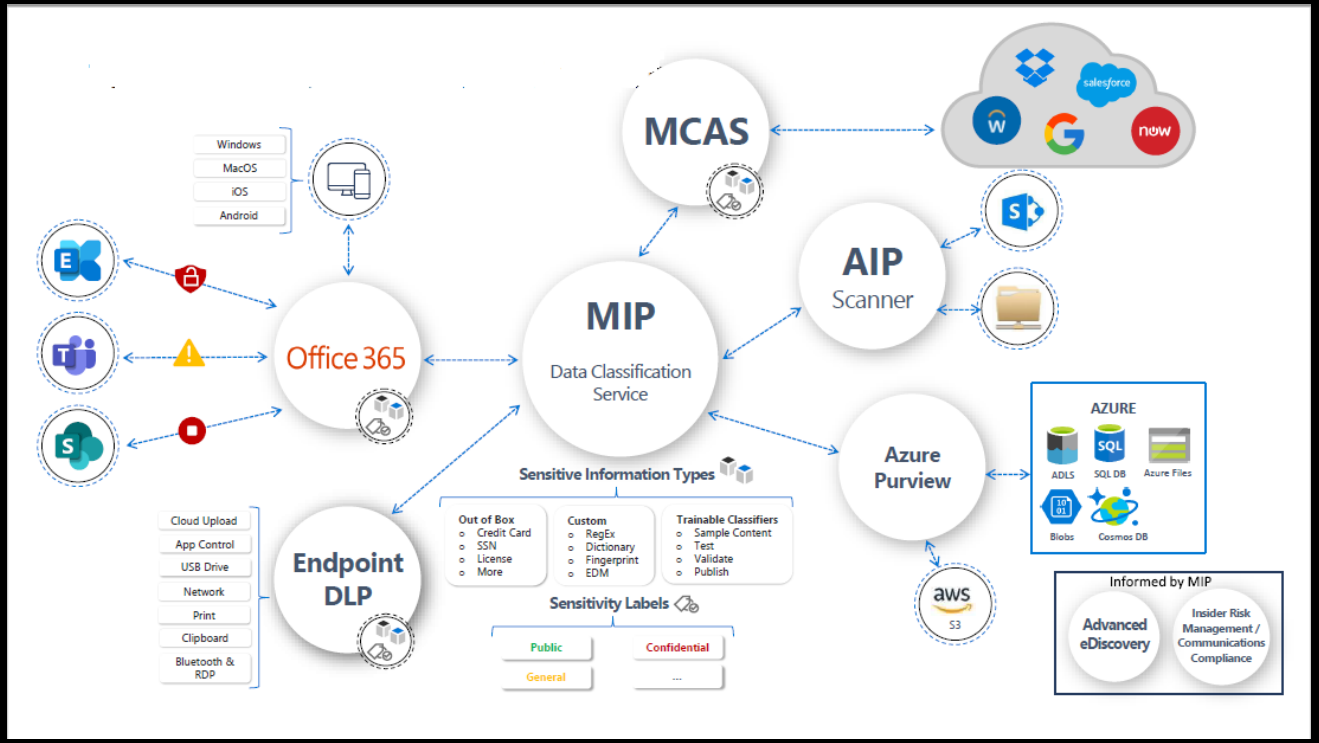
Data privacy regulations for information protection recommend:

- Protection against loss or unauthorized access, usage and/or transmission.
- Risk-based application of protective mechanisms.
- Use of encryption where appropriate.

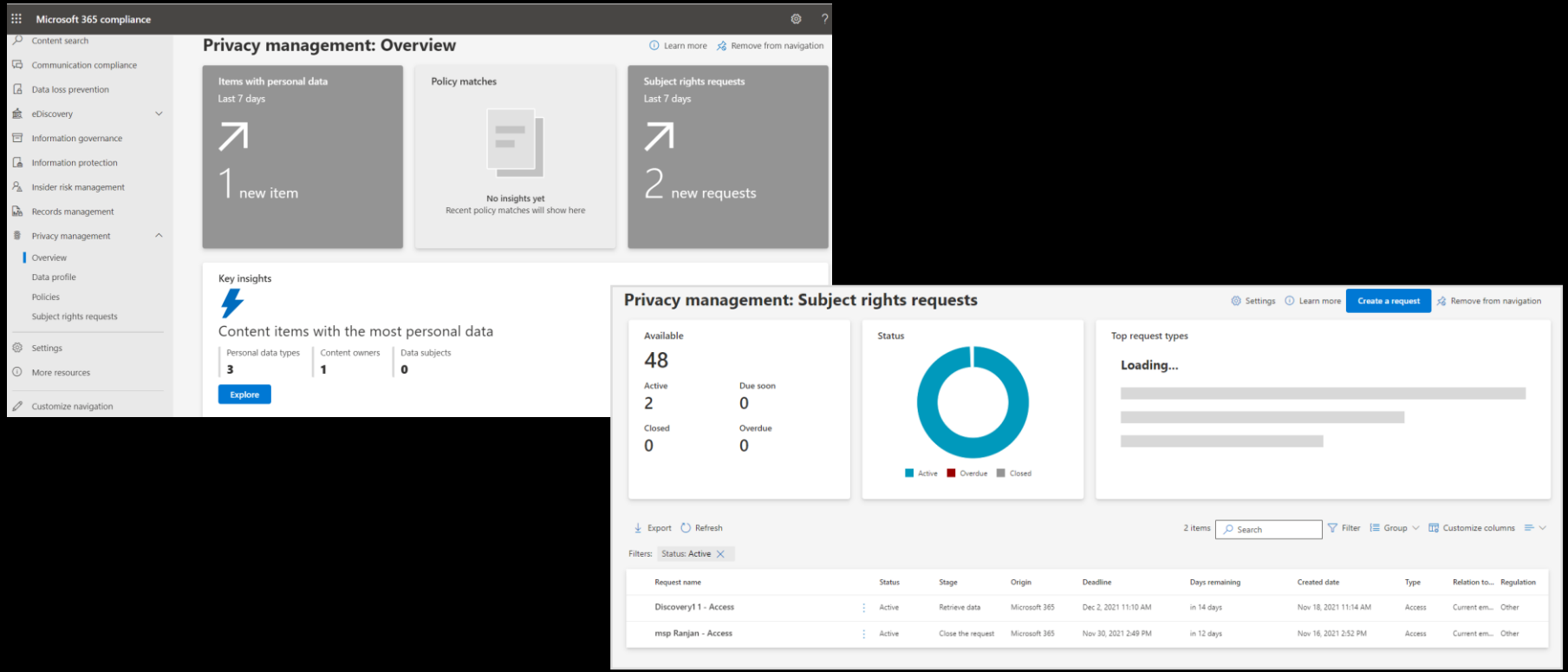
In Microsoft 365, information protection solutions include:

- Sensitive information types (described in the assess data privacy risks and identify sensitive items article)
- Sensitivity labels
  - Service/container-level
  - Client-side/content-level
  - Automated for data-at-rest in SharePoint and OneDrive
- Data Loss Prevention (DLP)
- Microsoft 365 Endpoint data loss prevention
- Office 365 Message Encryption new capabilities (OME) and OME Advanced Message Encryption

Discover & Protect information subject to data privacy regulation



Microsoft Priva – Privacy Risk Mgmt Portal Dashboard



Wipro's Privacy Mgmt Solution Stack & Maturity driven approach

Privacy Solutions for Transformation and Sustenance

Discover	Data Classification		Microsoft Priva, Microsoft M365 Compliance Suite Azure Purview
	Data Discovery		
	Data Mapping & Data Inventory	Data Retention and Disposal	
Manage	PIA/DPIAs	Privacy Threat Modelling	LINDDUN – Privacy Threat Modelling
	Consent and Choice	Cookie Consent	
	Individual Rights Management		
Protect	Encryption Management		Microsoft M365 Compliance Suite SNOW
	3rd Party Risks Management		
	Security Controls		
Record	Controls Assurance		
	Audits		
	Breach Management	Breach Notification and Reporting	SNOW
Report	Documentation	Dashboards and Reports	Microsoft Priva - Privacy Mgmt
	Certification		
	Code of Conduct		

Privacy Operations Center

Maturity Assessment

Wipro's Approach – By maturity

Baseline

- Identify PII processed by the Organization
- Build PII Inventory
- Build Privacy Policy and related privacy process and procedures
- Build privacy notices
- Conduct Gap Analysis/PIA
- Facilitate Data Subject Rights
- Maintain Records of Processing Activities
- Identify Privacy Risks and manage risks
- Manage consent and withdrawal of consent
- Manage Privacy Breach and notification
- Build privacy organization and governance
- Conduct Privacy Awareness and Training
- Conduct third party risk assessment.

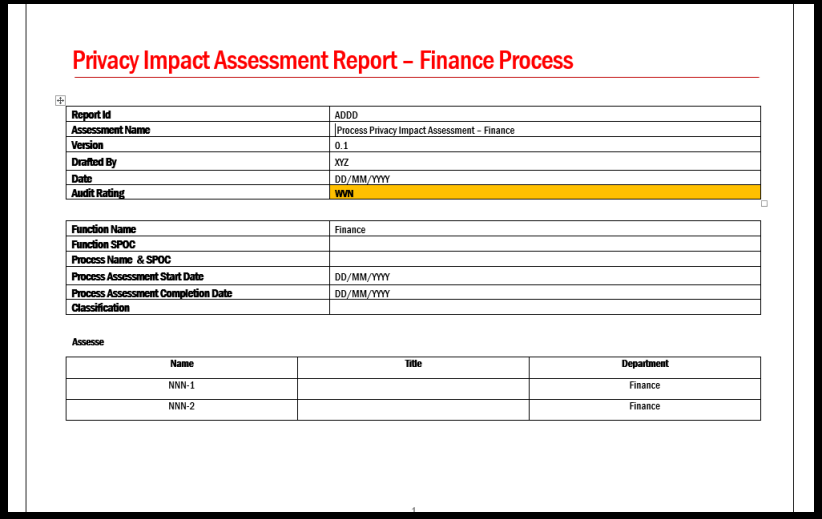
Advanced

- Automate identification and maintenance of PII inventory
- Implement policies and procedures using tools to prevent data leakage and safeguard data
- Automate PIA, manage privacy risks.
- Automate DPIA for process meeting criteria.
- Automate privacy risk management
- Automate Data Subject Access Requests fulfillment process
- Automate or implement tool for breach management and notification
- Automate Cookie Preference management
- Conduct Privacy Awareness and training at predefined frequency.
- Automate third party risk assessment
- Set up Privacy Operations Center

Optimal

- Privacy Impact Assessments for applications & business processes
- Privacy audits and data privacy control testing
- Privacy awareness through gamification and online campaigns
- Data Subject Access Requests fulfillment
- Privacy by Design Audits, Privacy by Design guidance to business stakeholders.
- Build Regulatory and Compliance Intelligence
- Setup Privacy Operations center to manage updates to privacy policies, processes, conduct regular PIA, DPIA and audits, respond to privacy related queries from business and application teams.

Sample PIA Reports



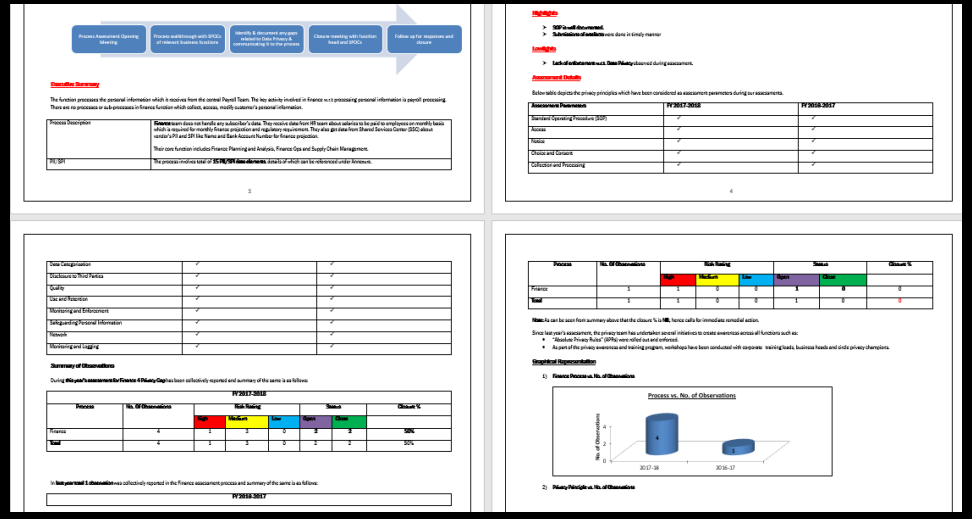
Privacy Impact Assessment Report – Finance Process

Report Id	ADDD
Assessment Name	Process Privacy Impact Assessment – Finance
Version	0.1
Drafted By	XYZ
Date	DD/MM/YYYY
Audit Rating	WVN

Function Name	Finance
Function SPOC	
Process Name & SPOC	
Process Assessment Start Date	DD/MM/YYYY
Process Assessment Completion Date	DD/MM/YYYY
Classification	

Assesse

Name	Title	Department
NNN-1		Finance
NNN-2		Finance



Process Assessment Opening Meeting | Process walkthrough with SPOCs of relevant business functions | Identify & document any gaps related to Data Privacy & communicating it to the process | Closure meeting with function head and SPOCs | Follow up for responses and closure

Executive Summary

The function processes the personal information which it receives from the central Payroll Team. The key activity involved in finance w.r.t processing personal information is payroll processing. There are no processes or sub-processes in finance function which collect, access, modify customer's personal information.

Process Description	**Finance** team does not handle any subscriber's data. They receive data from HR team about salaries to be paid to employees on monthly basis which is required for monthly finance projection and regulatory requirement. They also get data from Shared Services Center (SSC) about vendor's PII and SPI like Name and Bank Account Number for finance projection. Their core function includes Finance Planning and Analysis, Finance Ops and Supply-Chain Management.
PII, SPI	The process involves total of **15 PII/SPI data elements**, details of which can be referenced under Annexure.

Highlights

- **SOP is well documented.**
- **Submissions of assessments** were done in timely manner

Lowlights

- **Lack of enforcement w.r.t. Data Privacy** observed during assessment.

Assessment Details

Below table depicts the privacy principles which have been considered as assessment parameters during our assessments.

Assessment Parameters	FY 2017-2018	FY 2016-2017
Standard Operating Procedure (SOP)	✓	✓
Access	✓	✓
Notice	✓	✓
Choice and Consent	✓	✓
Collection and Processing	✓	✓

Data Categorisation	✓	✓
Disclosure to Third Parties	✓	✓
Quality	✓	✓
Use and Retention	✓	✓
Monitoring and Enforcement	✓	✓
Safeguarding Personal Information	✓	✓
Network	✓	✓
Monitoring and Logging	✓	✓

Summary of Observations

During **this year's assessment for Finance 4 Privacy Gap** has been collectively reported and summary of the same is as follows.

FY 2017-2018

Process	No. Of Observations	Risk Rating			Status		Closure %
		High	Medium	Low	Open	Close	
Finance	4	1	3	0	2	2	50%
Total	4	1	3	0	2	2	50%

In **last year total 1 observation** was collectively reported in the Finance assessment process and summary of the same is as follows.

FY 2016-2017

Process	No. Of Observations	Risk Rating			Status		Closure %
		High	Medium	Low	Open	Close	
Finance	1	1	0	0	1	0	0
Total	1	1	0	0	1	0	0

Note: As can be seen from summary above that the closure % is **NIL**, hence calls for immediate remedial action.

Since last year's assessment, the privacy team has undertaken several initiatives to create awareness across all functions such as:

- "Absolute Privacy Rules" (APRs) were rolled out and enforced.
- As part of the privacy awareness and training program, workshops have been conducted with corporate training leads, business heads and circle privacy champions.

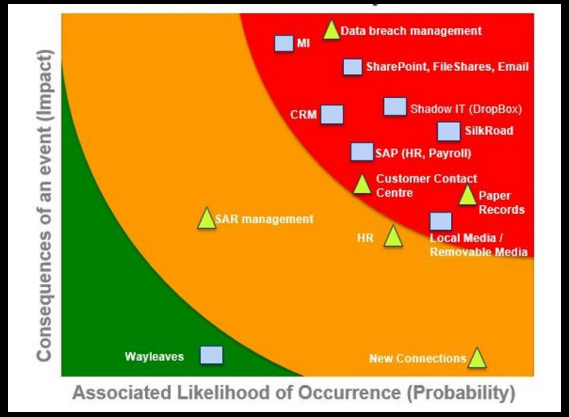
Graphical Representation

1) **Finance Process v. No. of Observations**

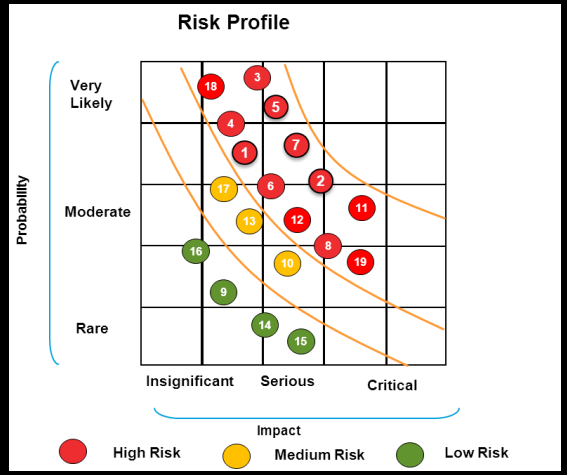
2) **Privacy Principle v. No. of Observations**

Sample Reports

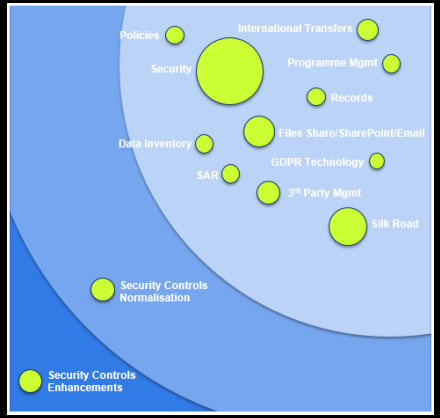
Risk Exposure

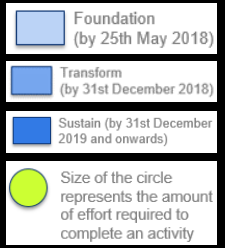


Gap Analysis Dashboard



High Level Roadmap





Key Privacy Case Studies - Think Privacy – Think Wipro

Thank you

wipro

CyberSecurity
by CyberSecurists.