happiest minds
The Mindful IT Company
Born Digital . Born Agile

Happiest Minds

GDPR Compliance Services (powered by Microsoft)

Nov 2021

happiest minds
The Mindful IT Company
Born Digital . Born Agile

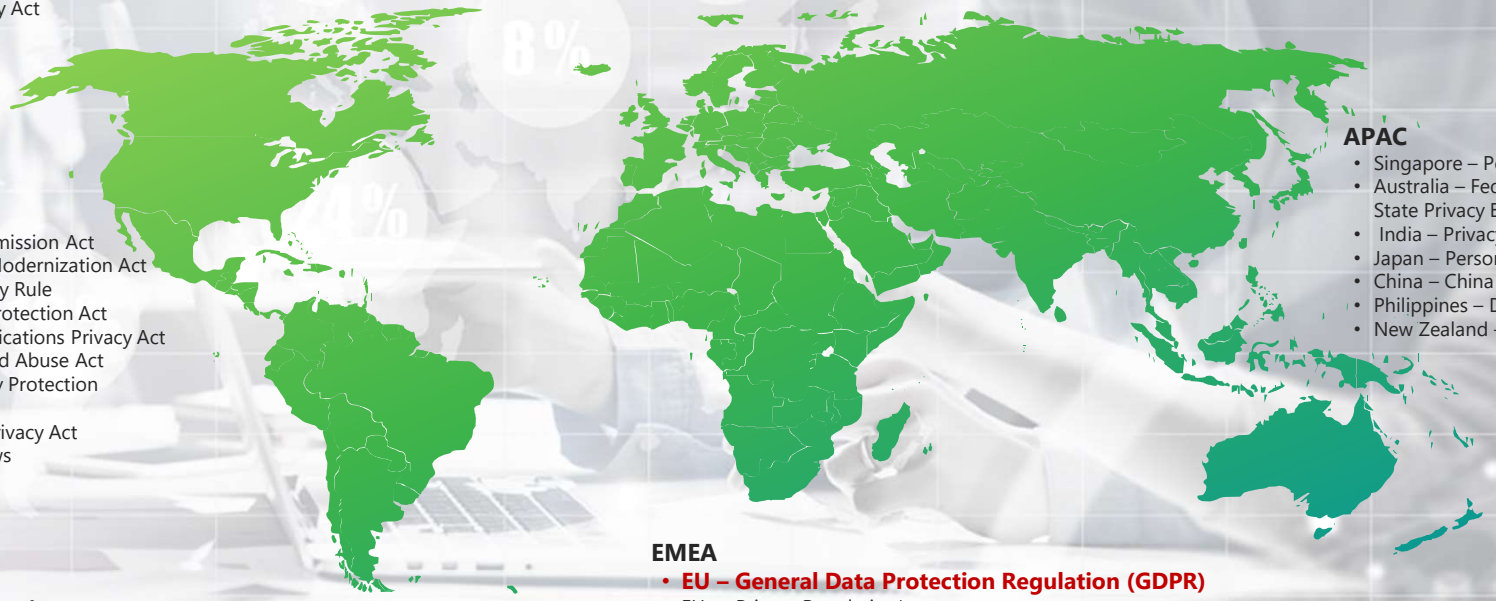
GDPR

Introduction & Challenges

Global privacy regulatory landscape is complex

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Canada
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Personal Information Protection Act (PIPA)
- Personal Information Protection and Identity Theft Prevention Act (PIPITPA)
- Quebec Privacy Act



United States
- The Federal Trade Commission Act
- The Financial Services Modernization Act
- HIPAA Privacy & Security Rule
- Telephone Consumer Protection Act
- The Electronic Communications Privacy Act
- The Computer Fraud and Abuse Act
- California Online Privacy Protection
- Texas Identity Theft Act
- California Consumers Privacy Act
- Other state's privacy laws

APAC
- Singapore – Personal Data Protection Act 2011
- Australia – Federal Privacy Amendment Bill & State Privacy Bills
- India – Privacy Rules 2011
- Japan – Personal Information Protection Act
- China – China Privacy & Cybersecurity Law
- Philippines – Data Privacy Act 2011
- New Zealand – Privacy Act 1993

Latin America
- Mexico – Federal Law on protection of personal data
- Argentina – Regulation 60, Data Protection Law 2000
- Brazil – Data Protection Bill

EMEA
- **EU – General Data Protection Regulation (GDPR)**
- EU – ePrivacy Regulation*
- UK – Privacy & Electronic Communications Regulations 2003
- France – Digital Republic Act
- Germany – Federal Data Protection Act
- Netherlands – Dutch notification of Data Breach Law
- Italy – Personal Data Protection Code
- Various other EU member states data protection laws

* Will complement GDPR as regards electronic communications data that qualify as personal data

EU GDPR introduces further new challenges

To understand the details and nature of data breach and notify DPA within 72 hours of data breach incident

Need to identify and inventory processes and systems handling personal information and maintain audit trails of processing activities for all data subjects

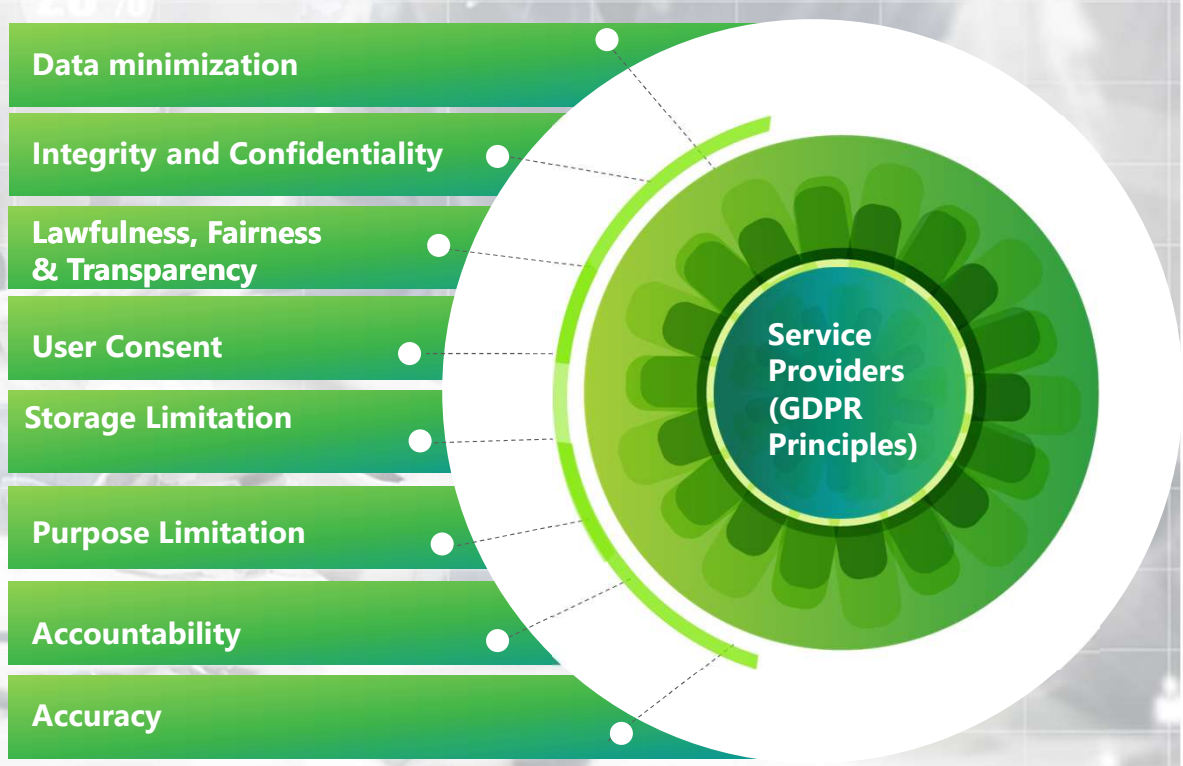
Significant additional resources need to be allocated to develop an effective data privacy assessment program and to implement privacy controls in service and development lifecycle

Implement technical controls to pseudonymize, encrypt, or otherwise secure personal data and maintain ongoing CIA of personal data

Re-negotiation of third-party contracts to enable compliance and management of contract inventory

Data subjects have rights to be forgotten and can request personal data to be rectified or to be transferred to any party, including competitors

What does it mean to end users and Service Providers?



Our GDPR Service

Offerings & Approach

OUR GPDR APPROACH powered by Microsoft

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Customer GDPR Compliance Journey

ASSESS

Assess GDPR Compliance for Overall Enterprise & specific Platforms & Applications -
Scope & Applicability determination, stakeholder mapping, Data flow mapping
Conduct GDPR Gap assessment and Provide Process & Technical - Recommended Action Plan (Phased & Time-Bound)

PROCESS REMEDIATION

Design required policies & processes – Privacy Policy, Data Subject Request Handling Procedures, Data Processors & Third-Party Agreement Templates, Data Breach Response procedures, registers, forms, templates, etc. to ensure customer endorses and complies with Applicable GDPR principles

TECHNICAL REMEDIATION

Ensure Privacy by Design & Default and implement PII Data Protection & Loss Prevention Solutions
Technical Guidance on data privacy principles – data minimization, data protection, etc.
Implement Sensitive Data discovery & classification, Message Encryption, DLP, least-privileged access controls, Incident management

ASSURANCE TESTING

Assurance of GDPR transformation program
Data Breach Simulation
Sampling and testing for Data Subject request for rights like data access, data erasure or modification
Conduct Staff Awareness Sessions
Responsibility change awareness

CONTINUED COMPLIANCE

Continued compliance with newly introduced changes
GDPR compliance incorporated into BAU processes.
Data Privacy Officer (DPO) services
Ongoing Data Privacy Impact Assessments
Ongoing Training and Awareness sessions
Suggestions for continuous improvements

Our Services enabled with Microsoft Security Solutions for GDPR Technical Compliance

DISCOVER & CLASSIFY

Identify, locate & classify personal data
M365
- Content Search
- Core eDiscovery
- Advanced eDiscovery
- Microsoft Information Protection Sensitivity Labels & AIP

PROTECT & MANAGE

Govern & manage how personal data is used and accessed
Azure AD
- RBAC - Access Controls
- Conditional Access Policies
- Privileged Identity Management

M365
- Data Loss Prevention
- DLP for Endpoint
- Retention Labels

Security Controls to protect sensitive data & identify data breach.
Microsoft Defender
- Defender for O365
- Defender for Cloud Apps
- Defender for Endpoint

Microsoft Endpoint Manager
- Intune
- Bitlocker Encryption

O365 Message Encryption

MONITOR & REPORT

Manage audit & compliance documentation & reporting
- **Compliance manager to** manage regulatory compliance activities
- Auditing and Alert Policies in the **Security and Compliance Center**
- **Insider Risk Management** policies
- **DSR Case tool for** DSR Response Management

Our GPDR Compliance Services powered by Microsoft

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Our Sensitive Data Security Services enabled with Microsoft Security Solutions for GDPR Technical Compliance

DEFINE → **DESIGN** → **DEPLOY** → **DRIVE**

DISOVER & CLASSIFY DATA

Identify, locate & classify personal data

Content Search can be used to search text and metadata in content across SharePoint Online, OneDrive for Business, and Exchange Online, etc.
This features also supports while responding to DSRs.
Core eDiscovery enables discovery case management
Advanced eDiscovery leverages ML for quick & precise documents identification
Microsoft Information Protection Sensitivity Labels & AIP to classify the data with various labels & levels of protection on emails, files or sites.

PROTECT & MANAGE DATA

Govern & manage how personal data is used, accessed & protected

Azure AD for Access controls
- RBAC - Access Controls
- Conditional Access Policies
- Privileged Identity Management

Data Loss Prevention to detect, warn, and block risky, inadvertent, or inappropriate sharing of sensitive data - Exchange Online, SharePoint, OneDrive, and Microsoft Teams & Office apps
Endpoint DLP for sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices
O365 Message Encryption to protect internal messages containing sensitive items.
OME Advanced to control sensitive emails shared externally with automatic policies that detect sensitive information types, expiry date & revocation.

Microsoft Endpoint Manager to manage devices
- Microsoft Intune – Device polices, App Protection polices, WIP
- Bitlocker for Disk Encryption

Microsoft Defender
- **Defender for O365** to protect against threats, detect malware, spams, etc. in emails, links & collaboration tools.
- **Defender for Cloud Apps** to provide visibility & control over data shared across cloud apps
- **Defender for Endpoint**

Retention Policies & Labels to retain or delete content in Microsoft 365 that contains or is expected to contain personal data.

MONITOR & REPORT

Manage audit & compliance documentation & reporting

Compliance manager to manage regulatory compliance activities, , get an overall score of org's current compliance configuration, and find recommendations for improvement.

Auditing and Alert Policies in the **Security and Compliance Center**

Insider Risk Management Policies

Data Subject Request Response Management via DSR Case tool in **Microsoft 365 compliance center**

End-to-End Solution Delivery – Solution Mapping & Definition, Configuration & Roll-out, Operate & Manage

Happiest Minds GDPR Service Enablers

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Metrics driven progress tracking, scope for automation and compliance change management	CONTINUOUS MATURITY ENHANCEMENT
Pre-engagement assessment leading to business context service delivery	CONTEXTUAL SERVICE DELIVERY
Deploying experienced consultants and accelerators to enable quick benefit realization	SPEEDING UP COMPLIANCE READY STATE
Drive synergies through consistent and integrated service delivery	UNLOCKING TRAPPED VALUE

Collaboration & Coordination	Integrated across enterprise ecosystem, enables seamless services experience
Agility & Value Realization	Drive value for Business, enhance user experience and brings business aligned agility
Simple & Sustainable	Focus on building fundamental capabilities, efficient approach to meeting objectives

Executing global compliance programs; certified Data Privacy & GDPR professionals; Raising Awareness

Strong technical expertise across DLP, Encryption & Masking, Endpoint Protection, SIEM & Incident management, etc.

Provide individuals to function as Regional Data Privacy Officer

Value we delivered to our clients

happiest minds
The Mindful IT Company
Born Digital . Born Agile

GDPR Assessment and Remediation

For a leading home shopping channel and online jewelry retailer in UK

- PI Data map formulation and gap assessment against applicable articles of GDPR
- Formulation of GDPR remediation roadmap and manage implementation of remediation plan
- Architecting DSR request management processes
- Draft GDPR-compliant privacy policy, incident & breach mgmt & contract agreements.
- DPO-as-a-Service

Timely and effective remediation of GDPR gaps identified across PII processing landscape, leading to GDPR regulatory compliant organizations

GDPR & CCPA Compliance Assessment

For global eCommerce platform provider.

- GDPR Compliance Assessment – Gaps Identification & Remediation Recommendation
- Remediation Implementation Assistance to become GDPR-compliant in quick time.
- Identification of differential controls between GDPR & CCPA
- Gap Assessment against applicable CCPA articles
- Suggest corrective measures to process & policy to become CCPA-compliant from already being GDPR-compliant.

Quick Guidance on becoming GDPR & CCPA-compliant

Records of Data Processing

For a leading energy enterprise in USA

- Inventory of PII business function, and associated IT systems, roles and third parties
- Tool based Data classification, Data flow map
- Data Security Awareness

Reduced Privacy regulation adoption time by >40%

Data Security Technology

For a global HR consulting firm in USA

- Identification of private and sensitive data across structured and unstructured file systems
- Data masking and encryption methodology
- Business rule-based implementation of the tool

100% achievement of PI data protection compliance requirement

Data Breach Management

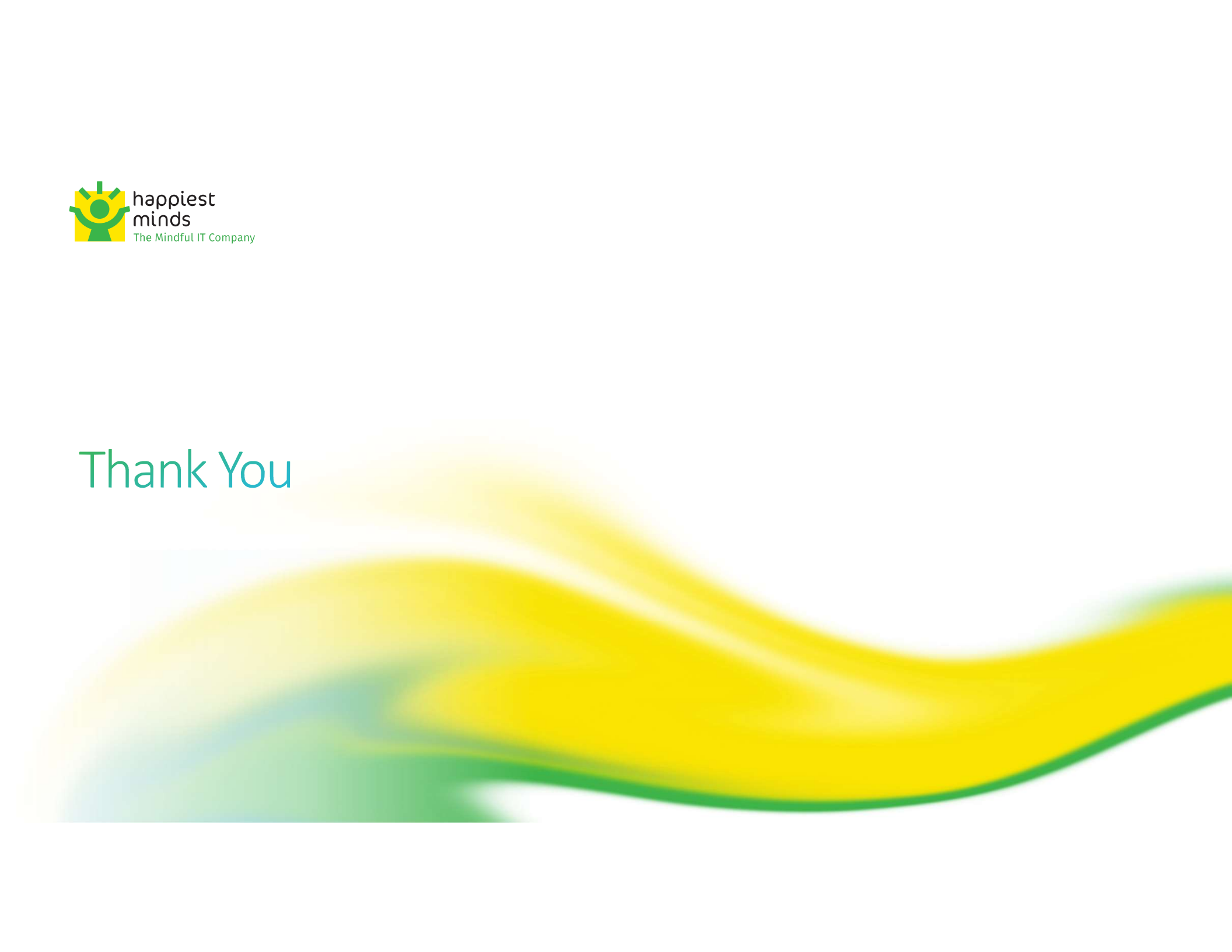
For a leading Telco and Oil Refinery Group in USA

- Security intelligence and incident response
- Analysis of logs and vulnerabilities
- Integration with enterprise risk management

Decreased or prevented >40% of breaches or attacks and reduced manual efforts

Next Steps

- A Consultative workshop to identify opportunities for Assessment and Remediation of GDPR
- Analysis and recommendations on the current stage of the privacy compliance of the targeted prospects
- Half a day workshop to understand the current GDPR compliance status and next steps
- Differential compliance assessment for GDPR-compliant customers to comply with other applicable privacy laws, viz. CCPA, etc.

happiest minds
The Mindful IT Company

Thank You