

Happiest Minds

CCPA / CPRA Compliance Services (powered by Microsoft)

CCPA / CPRA

Introduction & Challenges

Global privacy regulatory landscape is complex

Canada

- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Personal Information Protection Act (PIPA)
- Personal Information Protection and Identity Theft Prevention Act (PIPIPTA)
- 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**
- **California Privacy Rights Act**
- Virginia – Consumers Data Protection Act
- Other state's privacy laws

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

APAC

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

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

CCPA & CPRA introduce further new challenges

Complex privacy compliance requirements to be addressed within deadline



Breach Notification

To understand the details and nature of data breach and notify



Increased Record-keeping

Need to frame processes around handling personal information and maintain audit trails of processing requests for all data subjects



Implement Data Security

Implement technical controls to redact, aggregate, or otherwise secure personal data



Data Lifecycle Management

A completed Data inventory & map needs to be maintained. Also, process & systems to handle Data subjects' rights to opt-out deletion need to be designed



Third Party Risk Management

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



Privacy Impact Assessment

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

What's new in CPRA?

In June 2018, State of California Legislature passed **California Consumer Privacy Act (CCPA)** that went into effect from January 1 '2020.

CCPA applies to individuals and legal entities that do business in California. Impacts any business, whether in U.S., Europe, Asia or elsewhere who have customers located in California

It aims to strengthen consumer privacy rights and data protection.

The **California Privacy Rights Act (CPRA)** amends and expands CCPA, creating new requirements, consumer privacy rights, and enforcement mechanisms for applicable organizations.

The CPRA will come into effect **on January 1, 2023**. At that time, the CPRA will effectively replace the CCPA.

Till then, CCPA requirements will continue to apply to covered businesses.

New Sensitive Personal Information Category

New & Expanded Consumer Privacy Rights

Expanded Notification Requirements

Cyber Security Audit and periodic Risk Assessment Requirements

Incorporation of GDPR Principles – Data Minimization, Purpose Limitation, Storage Limitation

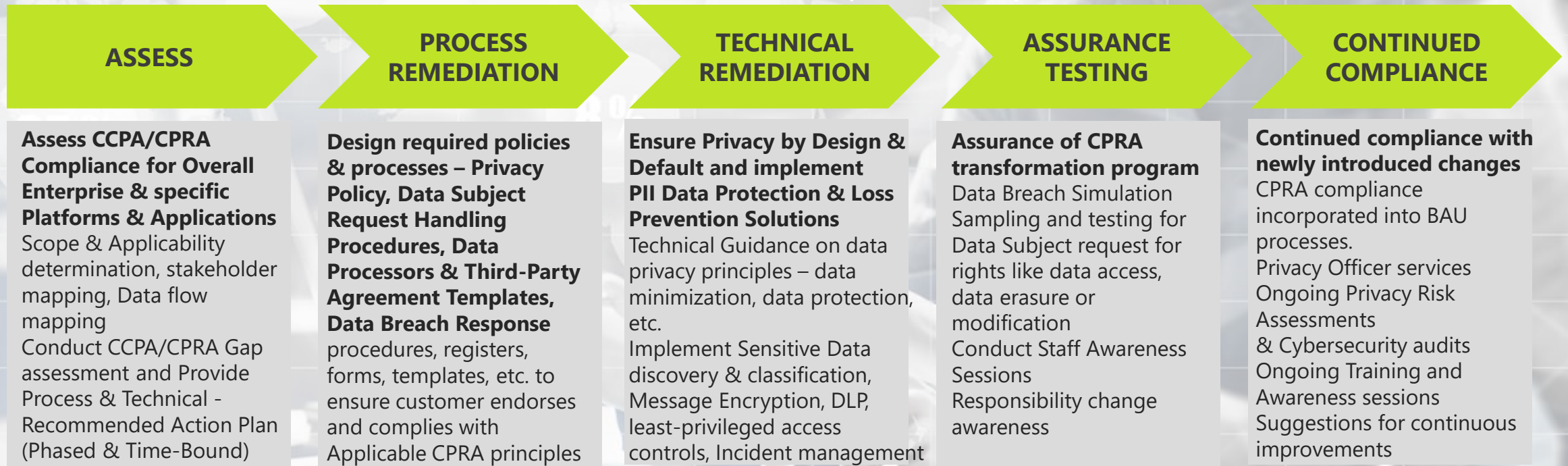
Expanded Private Right of Action

Creation of California Privacy Protection Agency (CPPA)

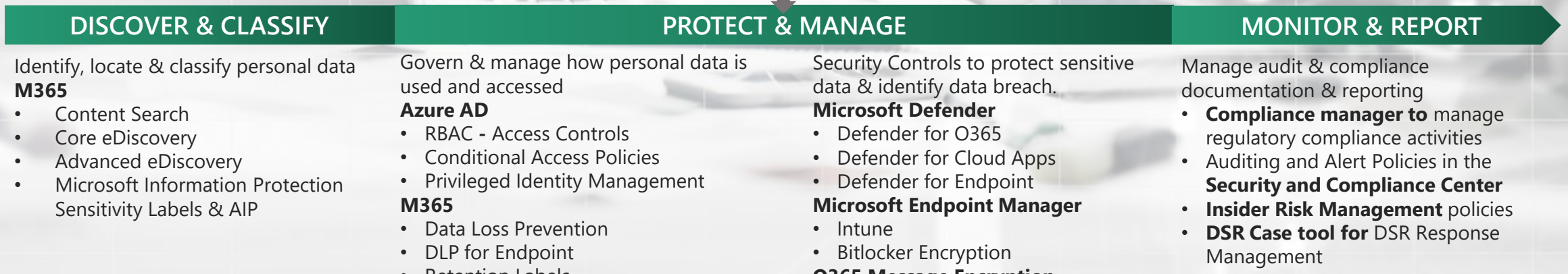
Our CCPA / CPRA Service Offerings & Approach

OUR CCPA / CPRA APPROACH powered by Microsoft

Customer CCPA / CPRA Compliance Journey



Our Services enabled with Microsoft Security Solutions for CCPA / CPRA Technical Compliance



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 CCPA / CPRA Compliance Services

powered by Microsoft

Our Sensitive Data Security Services enabled with Microsoft Security Solutions for CCPA / CPRA Technical Compliance

DEFINE

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.

DISCOVER & CLASSIFY DATA

DESIGN

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.

PROTECT & MANAGE DATA

DEPLOY

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

DRIVE

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.

Findings can be submitted to California Privacy Protection Agency (CPPA).

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 CCPA / CPRA Service Enablers



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

26%



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 & CCPA professionals; Raising Awareness

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

Provide individuals to function as Regional Data Privacy Officers

Value we delivered to our clients

CCPA Assessment and Remediation

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

- PI Data map formulation and gap assessment against applicable articles of CCPA
- Formulation of CCPA remediation roadmap and manage implementation of remediation plan
- Architecting DSR request management processes
- Draft CCPA-compliant privacy policy & contract agreements.
- Conducting CCPA Privacy training

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

CCPA Differential Gap Assessment

For global eCommerce platform provider.

- 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 CCPA-compliant

Data Security Risk Assessment

For a leading marketing analytics enterprise

- Complete Data Security Risk Assessment
- Data Security Requirements Definition & Product Evaluation
- Inventory of PII business function, and associated IT systems, roles and third parties
- Data Security Awareness

Reduced Privacy regulation adoption time by >40%

Data Security Technology

For a global HR consulting firm in USA

- Data Security Assessment
- 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 & Information Security Assessment

For a leading online gaming company for all its gaming platforms

- Overall security assessment across all security domains
- Data Security assessment for On-prem as well as cloud data centres
- Detailed Gap analysis & remediation recommendation
- Phased Roadmap

Practical action plan towards privacy & security posture strengthening

Next Steps

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

Thank You

