NEW WORLD OF WORK IS DRIVING CHANGE

41% of employees say mobile business apps change how they work
85% of enterprise organizations keep sensitive information in the cloud
88% of organizations no longer have confidence to detect and prevent loss of sensitive data
58% Have accidentally sent sensitive information to the wrong person

COMPLIANCE IS TOP-OF-MIND

50% year over year growth rate in electronic data
41% of organizations state enforcing of governance is their biggest issue
45% of organizations state lack of governance opens them to security and compliance risks

"My data is scattered across sources and the data continues to grow."
"I can’t apply unified policies across various data sources or to a specific repository."
"When enforcing compliance our business user productivity is disrupted."
"I want data governance to be automatic, not something I have to think about."
"How do I protect sensitive information such as sensitive PII data across my enterprise?"
"How do I find only relevant data when I need it?"
Providing clarity and consistency for the protection of personal data

The General Data Protection Regulation (GDPR) imposes new rules on organizations in the European Union (EU) and those that offer goods and services to people in the EU, or that collect and analyze data tied to EU residents, no matter where they are located.

- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance

Microsoft believes the GDPR is an important step forward for clarifying and enabling individual privacy rights.

What are the key changes to address the GDPR?

- **Personal privacy**: Individuals have the right to access their personal data, correct errors in their personal data, erase personal data, and obtain personal data.
- **Controls and notifications**: Organizations will need to provide clear notice of data collection, outline processing purposes and use cases, define data retention and deletion policies, and train privacy personnel.
- **Transparent policies**: Organizations are required to provide clear notice of data collection, outline processing purposes and use cases, define data retention and deletion policies, and train privacy personnel.
- **IT and training**: Organizations will need to protect personal data using appropriate security, notify authorities of personal data breaches, obtain appropriate consents for processing data, and keep records detailing data processing.

What does this mean for my data?

- **Better data governance** to provide control to data subjects and ensure lawful processing.
How do I get started?

1. Discover
   Identify what personal data you have and where it resides

2. Manage
   Govern how personal data is used and accessed

3. Protect
   Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches

4. Report
   Keep required documentation, manage data requests and breach notifications

GENERAL DATA PROTECTION REGULATION (GDPR)

- Enhanced personal privacy rights
- Increased duty for protecting data
- Mandatory breach reporting
- Significant penalties for non-compliance

HOW YOU GET STARTED:

1. Discover
   Identify what personal data you have and where it resides

2. Manage
   Govern how personal data is used and accessed

3. Protect
   Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches

4. Report
   Keep required documentation, manage data requests and breach notifications

HOW DO I PROTECT SENSITIVE INFORMATION?

INFORMATION PROTECTION LIFECYCLE

Detect
Scan & detect sensitive data based on policy

Classify
Classify data and apply labels based on sensitivity

Protect
Apply protection actions, including encryption, access restrictions

Monitor
Reporting, alerts, remediation
Detect SENSITIVE INFORMATION
No matter where it’s created, modified or shared
CLASSIFY INFORMATION BASED ON SENSITIVITY

Automatic classification:
Policies can be set by IT Admins for automatically applying classification and protection to data.

Recommended classification:
Based on the content you're working on, you can be prompted with suggested classification.

Manual reclassification:
You can override a classification and optionally be required to provide a justification.

User-specified classification:
Users can choose to apply a sensitivity label to the email or file they are working on with a single click.

SENSITIVITY LABELS PERSIST WITH THE DOCUMENT

Document labeling - what is it?
Metadata written into document files.

Travels with the document as it moves:
In clear text so that other systems such as a DLP engine can read it.

Used for the purpose of apply a protection action or data governance action - determined by policy.

Can be customized per the organization's needs.

CLASSIFICATION & LABELING EXAMPLE - SENSITIVE DATA

Discover personal data and apply persistent labels:
Labels are persistent and readable by other systems e.g. DLP engine.
Label is metadata written to data
Sensitive data is automatically detected.
Detect  Classify  Protect  Monitor
Scan & detect sensitive data based on policy  Classify data and apply labels based on sensitivity  Apply protection actions, including encryption, access restrictions  Reporting, alerts, remediation

PROTECT SENSITIVE DATA ACROSS YOUR ENVIRONMENT

Cloud & on-premises
File encryption
Email encryption and rights protection
Permissions and rights-based restrictions
DLP actions to prevent sharing
Policy tips & notifications for end-users
Visual markings in documents
Control and protect data in cloud apps with granular policies and anomaly detection
Data retention, expiration, deletion

Devices
Drive encryption
Remote wipe
Business data separation
**MONITOR INFORMATION PROTECTION EVENTS FOR GREATER CONTROL**

**Visibility**
- Policy violations
- Document access & sharing
- App usage
- Anomalous activity
- End-user overrides
- False positives

**Take Action**
- Tune & revise policies
- Revoke access
- Quarantine file
- Quarantine user
- Integrate into workflows & SIEM

**MICROSOFT'S INFORMATION PROTECTION SOLUTIONS**

Comprehensive protection of sensitive data throughout the lifecycle – inside and outside the organization

**DEVICES**
- PCs, tablets, mobile
- Office 365 DLP
- Windows Information Protection & BitLocker for Windows 10
- Azure Information Protection
- Exchange Online, SharePoint Online & OneDrive for Business
- Highly regulated
- Intune MDM & MAM for iOS & Android

**CLOUD**
- Azure 3rd-Party SaaS
- Office 365 Advanced Data Governance
- Microsoft Cloud App Security

**ON PREMISES**
- Datacenters, file shares
- Microsoft Cloud App Security

**Detect**
**Classify**
**Protect**
**Monitor**
5 Steps Program

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Classify</td>
<td>Take simple steps, it generates high-impact quickly (i.e. ‘Do Not Forward’ for HR and Legal)</td>
</tr>
<tr>
<td>2. Label</td>
<td>Test, phase the roll out, and learn – IT can’t know it all</td>
</tr>
<tr>
<td>3. Protect</td>
<td>Control sensitive internal email flow across all PCs/Devices</td>
</tr>
<tr>
<td>4. Monitor</td>
<td>‘Share Protected’ files with business partners (B2B)</td>
</tr>
<tr>
<td>5. Respond</td>
<td>Teach and enable users to revoke access</td>
</tr>
</tbody>
</table>

Thank you!