GDPR Compliance - Roadmap and Tools

Dominique Aboudaram – Partner
aboudaram@ttt.ch
What does GDPR mean for my data?

- Stricter control on where personal data is stored and how it is used
- Improved data policies to provide control to data subjects and ensure lawful processing
- Better data governance tools for better transparency, recordkeeping and reporting

Protecting customer privacy with GDPR
Uncover risk and take action

Discover data across systems
- Easily discover and catalog data sources
- Increase visibility with auditing capabilities
- Identify where personal info resides across devices, apps and platforms

Govern access and processing
- Enforce use policies and access controls across your systems
- Classify data for simplified compliance
- Easily respond to data requests and transparency requirements

Protect through the entire lifecycle
- Protect user credentials with risk-based conditional access
- Safeguard data with built-in encryption technologies
- Rapidly respond to intrusions with built-in controls to detect and respond to data breaches
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
Case Study
GDPR & Microsoft
Why Microsoft Cloud for this case study

Many federations already use it

Commitment to GDPR
Compliance of the platform, and many available tools

Global management
Data classification, Discovery, Security Policy, Compliance portal...
Microsoft Ecosystem to
PREPARE FOR THE GDPR
1. **Discover:**
Identify what personal data you have and where it resides

**In-scope:**
Any data that helps you identify a person
- Name
- Email address
- Social media posts
- Physical, physiological, or genetic information
- Medical information
- Location
- Bank details
- IP address
- Cookies
- Cultural identity

**Inventory:**
Identifying where personal data is collected and stored
- Emails
- Documents
- Databases
- Removable media
- Metadata
- Log files
- Backups

---

**Example solutions**

- **Microsoft Azure**
  Microsoft Azure Data Catalog
- **Enterprise Mobility + Security (EMS)**
  Microsoft Cloud App Security
- **Dynamics 365**
  Audit Data & User Activity
  Reporting & Analytics
- **Office & Office 365**
  Data Loss Prevention
  Advanced Data Governance
  Office 365 eDiscovery
- **SQL Server and Azure SQL Database**
  SQL Query Language
- **Windows & Windows Server**
  Windows Search
Data Subject access rights

Identify - report

Provide a report

DSR cases

Identify all data related to one person

DSR Follow-up

Active & closed cases from past 60 days
2 Manage:
Govern how personal data is used and accessed within your organization

Data governance:
Defining policies, roles and responsibilities for the management and use of personal data
- At rest
- In process
- In transit
- Storing
- Recovery
- Archiving
- Retaining
- Disposal

Data classification:
Organizing and labeling data to ensure proper handling
- Types
- Sensitivity
- Context / use
- Ownership
- Custodians
- Administrators
- Users

Example solutions

Microsoft Azure
Azure Active Directory
Azure Information Protection
Azure Role-Based Access Control (RBAC)

Enterprise Mobility + Security (EMS)
Azure Information Protection

Dynamics 365
Security Concepts

Office & Office 365
Advanced Data Governance
Journaling (Exchange Online)

Windows & Windows Server
Microsoft Data Classification Toolkit
Data Classification

Label & retention policies

Create a label to help users classify their content.

- Name your label

Label settings

Retention
- On

When this label is applied to content...
- Retain the content
  - For this long... 7 years
- Don’t retain the content, just delete it if it’s older than
  - 3 years

Retain or delete the content based on when it was labeled

Classify Data & groups with labels

Apply retention policies

Apply labels manually or automatically
Sharepoint GDPR Activity HUB

- Tracking of Events and Incidents
- Tracking of Requests from Data Subjects
- Tasks Assignment and Management for GDPR Processes
- Hierarchy of GDPR Roles in the Company
3 Protect:
Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches

Preventing data attacks:
Protecting your data
- Physical datacenter protection
- Network security
- Storage security
- Compute security
- Identity management
- Access control
- Encryption
- Risk mitigation

Detecting & responding to breaches:
Monitoring for and detecting system intrusions
- System monitoring
- Breach identification
- Calculating impact
- Planned response
- Disaster recovery
- Notifying DPA & customers

Example solutions
Microsoft Azure
- Azure Key Vault
- Azure Security Center
- Azure Storage Services Encryption

Enterprise Mobility + Security (EMS)
- Azure Active Directory Premium
- Microsoft Intune

Office & Office 365
- Advanced Threat Protection
- Threat Intelligence

SQL Server and Azure SQL Database
- Transparent data encryption
- Always Encrypted

Windows & Windows Server
- Windows Defender Advanced Threat Protection
- Windows Hello
- Device Guard
Multi-Factor Authentication

81% of hacking breaches leverage stolen and/or weak passwords

Available in all Subscriptions

Protects against the Number one problem: Identity theft

One click activations

Other brands propose it also (Gmail etc.)

Protect at the front door
### AIP – Protect sensitive data

#### Azure information protection Labels

<table>
<thead>
<tr>
<th>Label Display Name</th>
<th>Policy</th>
<th>Marking</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal</td>
<td>Global</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td>Global</td>
<td></td>
<td></td>
</tr>
<tr>
<td>General</td>
<td>Global</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential</td>
<td>Global</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All Employees</td>
<td>Global</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Anyone (not protected)</td>
<td>Global</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Recipients Only</td>
<td>Global</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Highly Confidential</td>
<td>Global</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Protection templates</td>
<td>Global</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Label with encryption
- Rules (do not forward, do not print, etc..)
- Follow up of documents
- Security in documents
Data Loss Protection

Define policy

Use Labels or sensitive data

Define block or alert policy

Review

Protect your sensitive content with DLP

Some docs in your org contain one or more DLP's most common types of sensitive information but aren't being protected by a DLP policy. Learn about our policy recommendations

DLP's top 5 sensitive info types that were detected in your content.

- Credit Card Number

To help protect the sensitive info listed above, we can set up a DLP policy that will:

- Detect when users share content from Exchange, SharePoint, and OneDrive that contains one of the unprotected types above.

- Generate detailed activity reports so you can track things like who shared the content with people outside your org and when they did it.

You can also turn on admin and user notifications. Don't worry...if you want to change these options later, you can edit the policy after it's created. You can even prevent people from sharing content if you like.

- Send me an email when users share a list of this sensitive info with people outside my org
- Add other users to the email
- Show a policy tip to users when they attempt to share this sensitive info with people outside my org

Create and apply policy  Cancel
EMS – Protection layers

MICROSOFT INTUNE
Make sure your devices are compliant and secure, while protecting data at the application level.

MICROSOFT CLOUD APP SECURITY
Gain deep visibility, strong controls and enhanced threat protection for data stored in cloud apps.

AZURE ACTIVE DIRECTORY
Ensure only authorized users are granted access to personal data using risk-based conditional access.

AZURE INFORMATION PROTECTION
Classify, label, protect and audit data for persistent security throughout the complete data lifecycle.

MICROSOFT ADVANCED THREAT ANALYTICS
Detect breaches before they cause damage by identifying abnormal behavior, known malicious attacks and security issues.
4 Report:
Keep required documentation, manage data requests and breach notifications

Record-keeping: Enterprises will need to record the:
- Purposes of processing
- Classifications of personal data
- Third-parties with access to the data
- Organizational and technical security measures
- Data retention times

Reporting tools: Implement reporting capabilities
- Cloud services (processor) documentation
- Audit logs
- Breach notifications
- Handling Data Subject Requests
- Governance reporting
- Compliance reviews

Example solutions
- Microsoft Trust Center
  Service Trust Portal
- Microsoft Azure
  Azure Auditing & Logging
  Azure Data Lake
  Azure Monitor
- Enterprise Mobility + Security (EMS)
  Azure Information Protection
- Dynamics 365
  Reporting & Analytics
- Office & Office 365
  Service Assurance
  Office 365 Audit Logs
  Customer Lockbox
- Windows & Windows Server
  Windows Defender Advanced Threat Protection
Compliance Manager

Plan and document your compliance status

https://servicetrust.microsoft.com/ComplianceManager
GDPR Management Platforms
One Trust – Comprehensive platform

https://www.onetrust.com/
One Trust – Risk Analytics
GDPR Workspace

https://www.values-associates.com/fr/
GDPR Workspace - Risks and remediation plans
Resources

• Microsoft.com/GDPR
• Microsoft Online Services and GDPR
  • Microsoft Azure
  • Office and Office 365
  • Microsoft Dynamics 365
  • Enterprise Mobility Suite
  • Windows and Windows Server
  • SQL Server
Questions?
Contact

Dominique Aboudaram – Partner – Technical Manager
aboudaram@ttt.ch

tel: +41 22 994 90 90
fax: +41 22 361 75 16

3T Technology Transfer & Training
Avenue du Mont Blanc 31
1196 Gland

ttt@ttt.ch