3T Technology Transfer & Training

GDPR Compliance - Roadmap and Tools

Dominique Aboudaram – Partner
aboudaram@ttt.ch

What does GDPR mean for my data?

Protecting customer privacy with GDPR

Stricter control on where personal data is stored and how it is used

Better data governance tools for better transparency, recordkeeping and reporting

Improved data policies to provide control to data subjects and ensure lawful processing

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

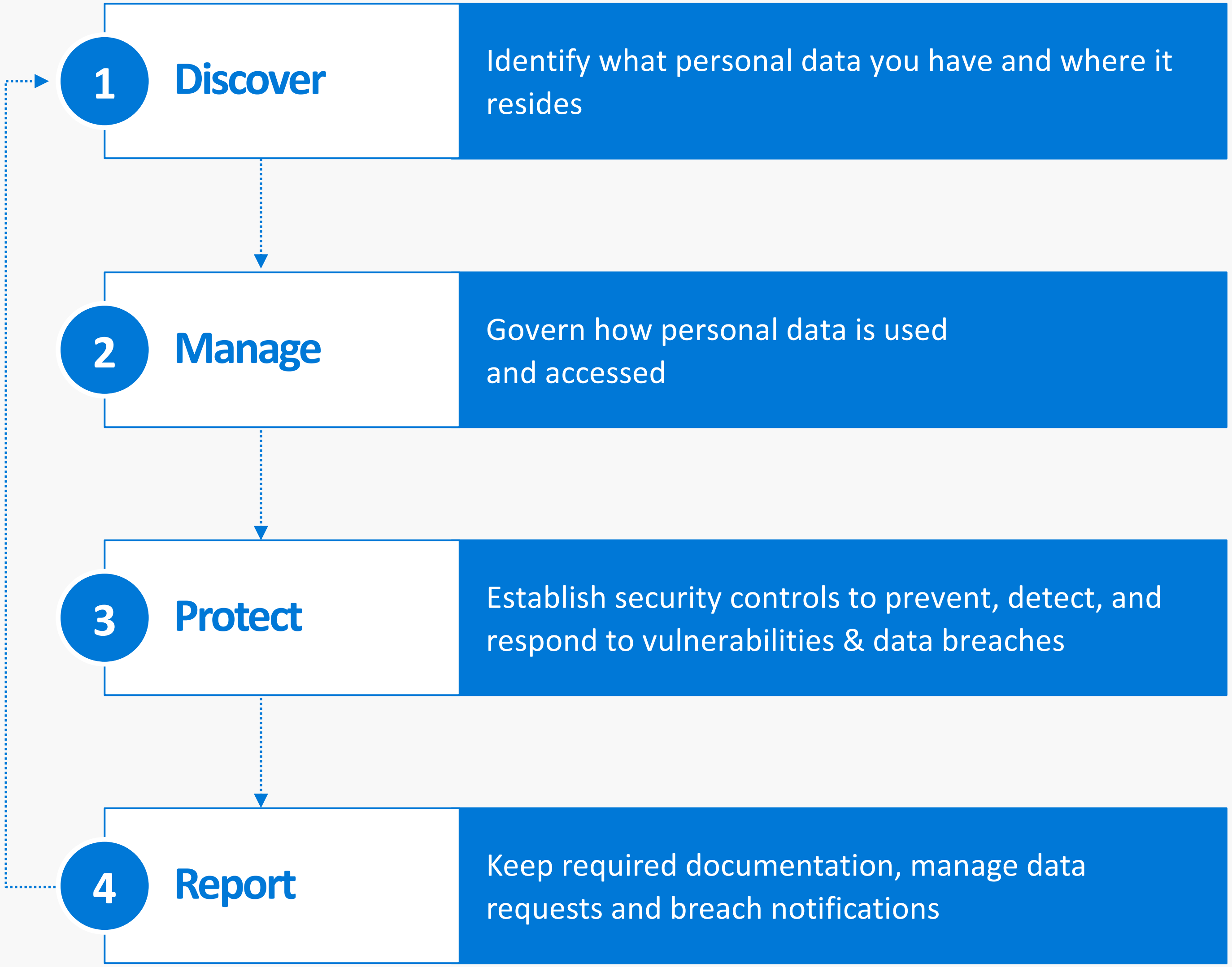
Govern access and processing

- 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

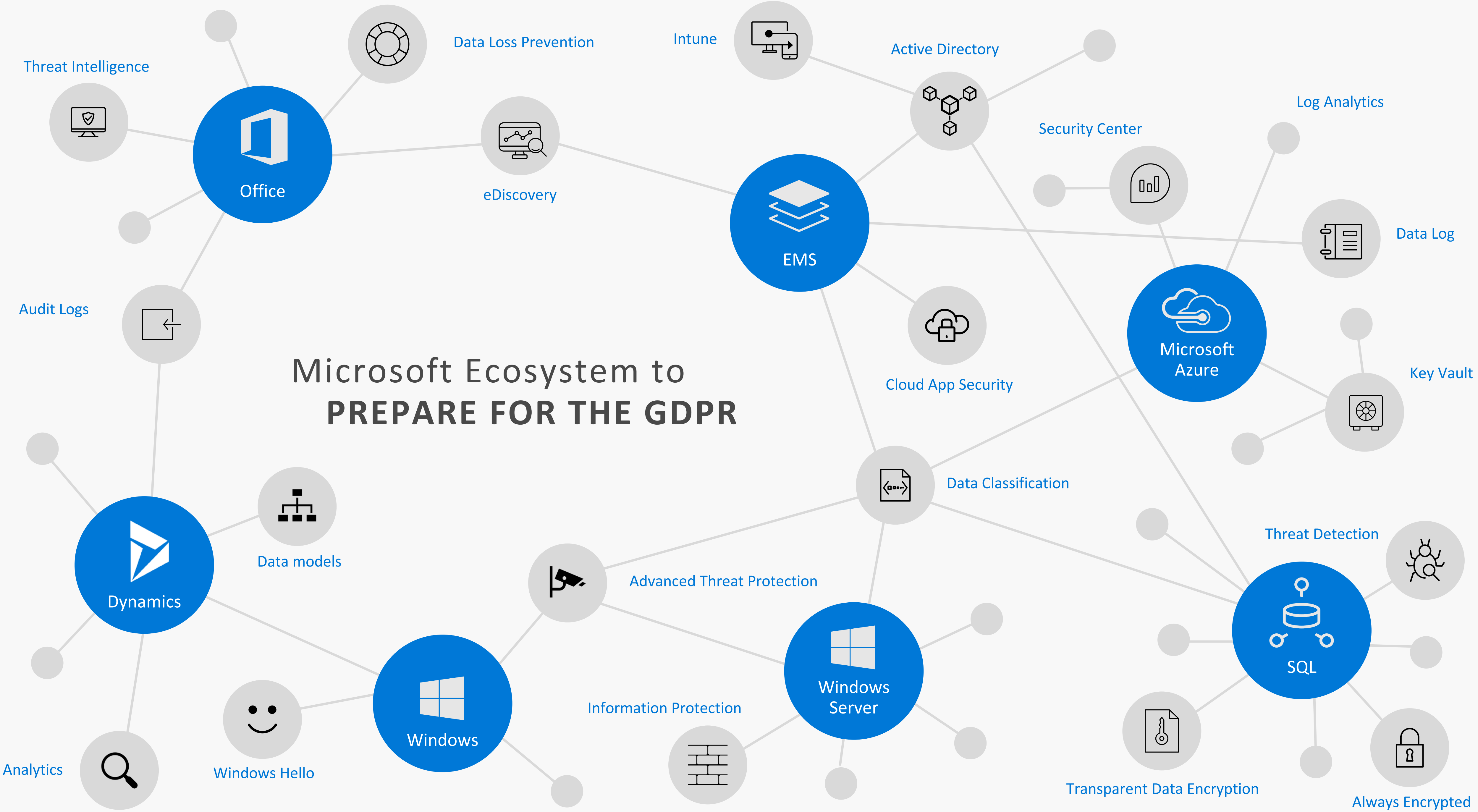
Commitment to GDPR

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

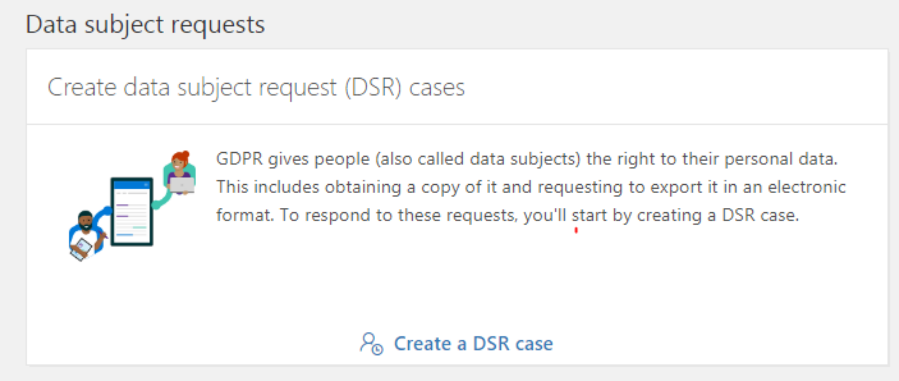
Windows Search

Data Subject access rights

Identify - report

Identify all data related to one person
Provide a report

DSR cases



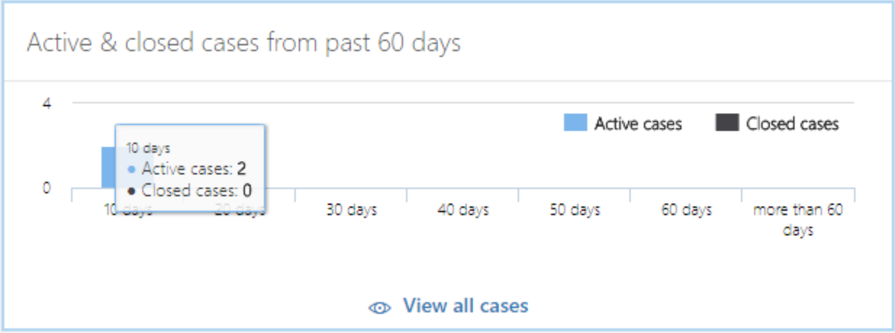
Data subject requests

Create data subject request (DSR) cases

GDPR gives people (also called data subjects) the right to their personal data. This includes obtaining a copy of it and requesting to export it in an electronic format. To respond to these requests, you'll start by creating a DSR case.

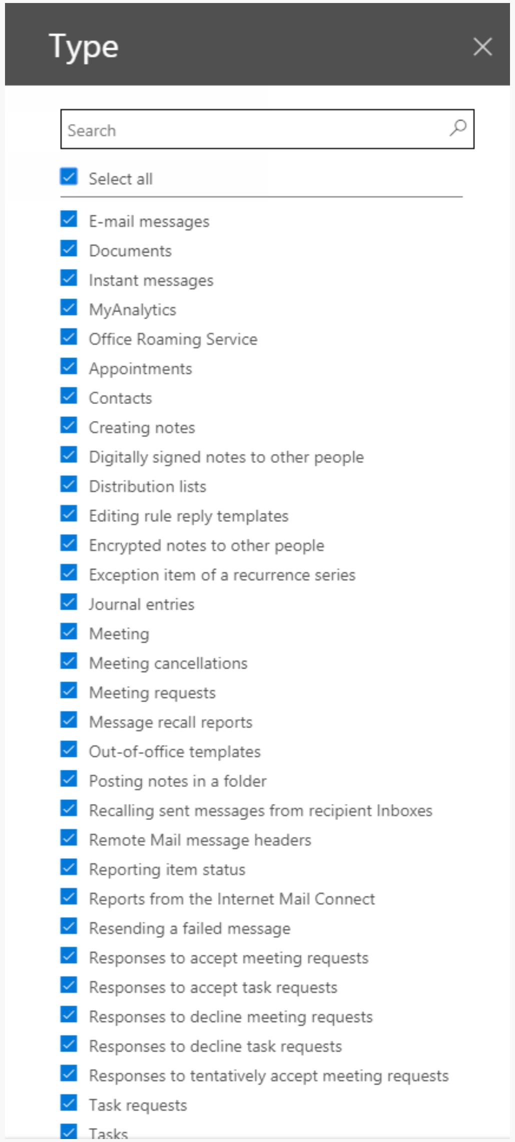
Create a DSR case

DSR Follow-up



Active & closed cases from past 60 days

View all cases



Type

Search

☑ Select all

☑ E-mail messages
☑ Documents
☑ Instant messages
☑ MyAnalytics
☑ Office Roaming Service
☑ Appointments
☑ Contacts
☑ Creating notes
☑ Digitally signed notes to other people
☑ Distribution lists
☑ Editing rule reply templates
☑ Encrypted notes to other people
☑ Exception item of a recurrence series
☑ Journal entries
☑ Meeting
☑ Meeting cancellations
☑ Meeting requests
☑ Message recall reports
☑ Out-of-office templates
☑ Posting notes in a folder
☑ Recalling sent messages from recipient Inboxes
☑ Remote Mail message headers
☑ Reporting item status
☑ Reports from the Internet Mail Connect
☑ Resending a failed message
☑ Responses to accept meeting requests
☑ Responses to accept task requests
☑ Responses to decline meeting requests
☑ Responses to decline task requests
☑ Responses to tentatively accept meeting requests
☑ Task requests
☑ Tasks

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

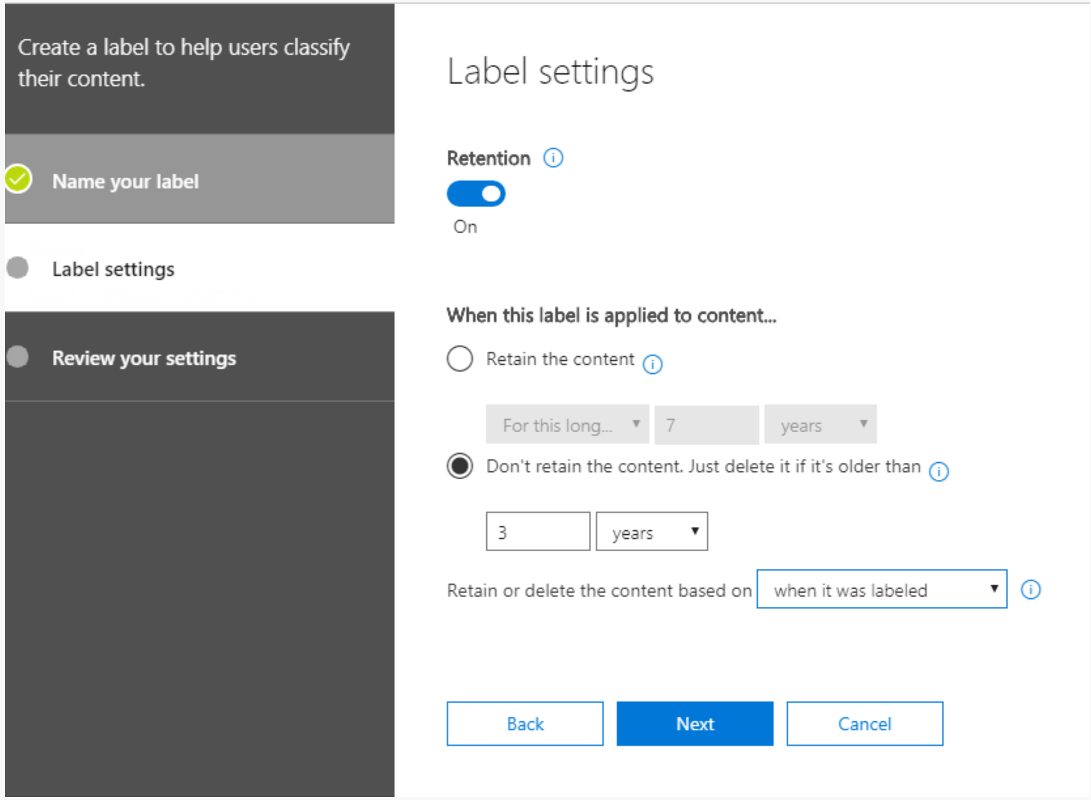
Advanced Data Governance
Journaling (Exchange Online)

Windows & Windows Server

Microsoft Data Classification Toolkit

Data Classification

Label & retention policies



Create a label to help users classify their content.

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 ▾

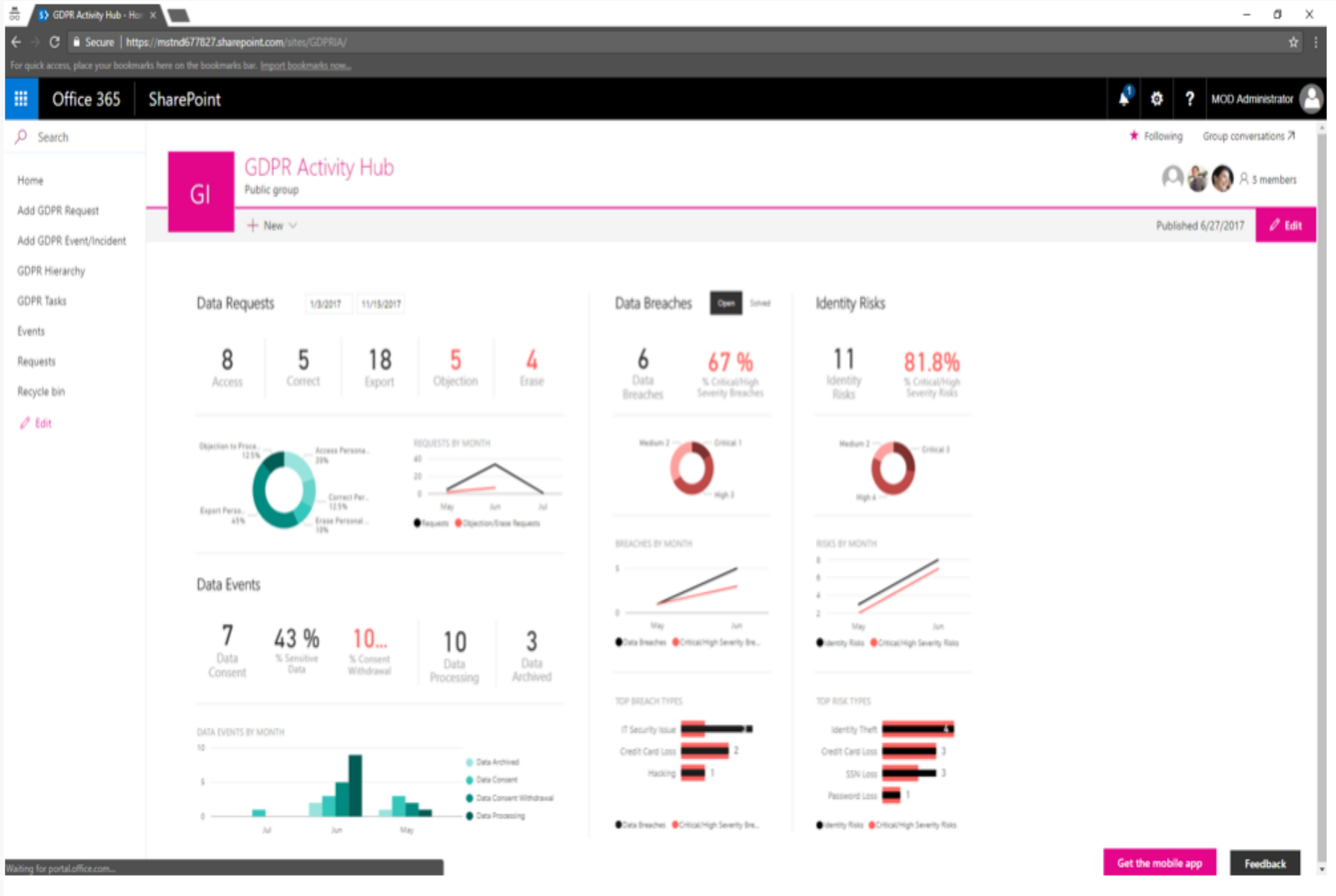
Retain or delete the content based on when it was labeled ▾ ⓘ

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

Protect at the front door

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

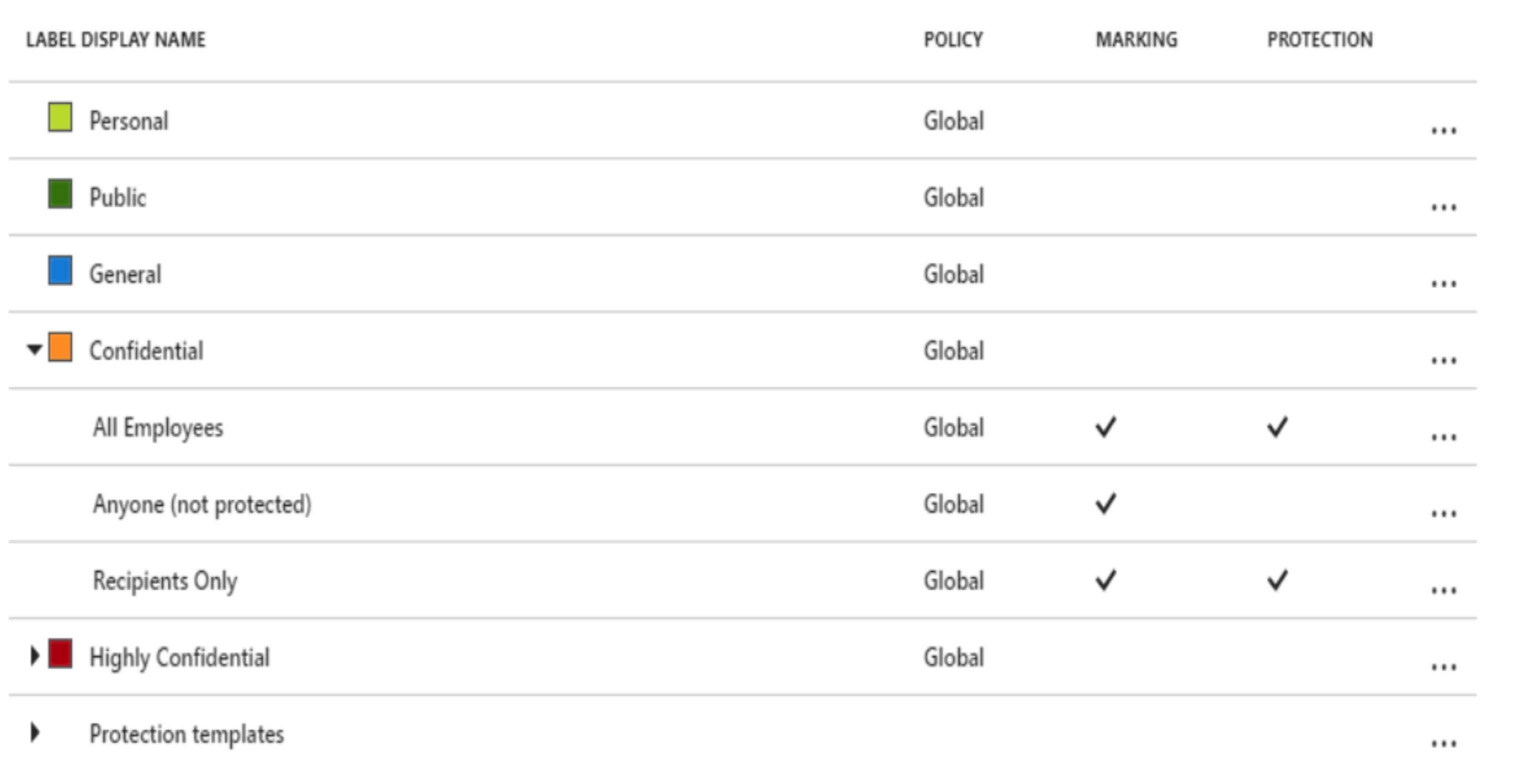
One click activations

Other brands propose it also (Gmail etc..)

Verizon - 207 Data Breach Investigation Report

AIP – Protect sensitive data

Azure information protection Labels



LABEL DISPLAY NAME	POLICY	MARKING	PROTECTION	
🟩 Personal	Global			...
🟩 Public	Global			...
🟦 General	Global			...
▾ 🟧 Confidential	Global			...
All Employees	Global	✓	✓	...
Anyone (not protected)	Global	✓		...
Recipients Only	Global	✓	✓	...
▸ 🟥 Highly Confidential	Global			...
▸ Protection templates				...

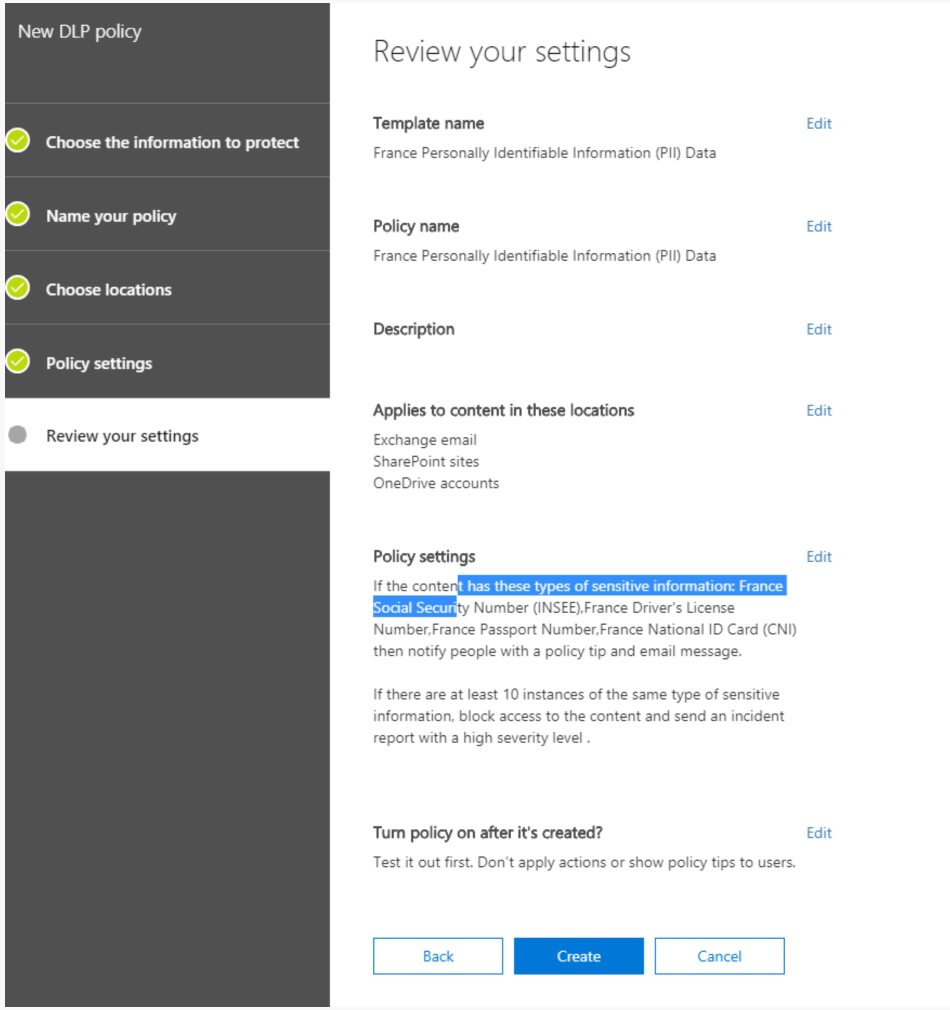
Label with encryption

Rules (do not forward, do not print, etc..)

Follow up of documents

Security in documents

Data Loss Protection



New DLP policy

- ✓ Choose the information to protect
- ✓ Name your policy
- ✓ Choose locations
- ✓ Policy settings
- ● Review your settings

Review your settings

Template name Edit

France Personally Identifiable Information (PII) Data

Policy name Edit

France Personally Identifiable Information (PII) Data

Description Edit

Applies to content in these locations Edit

Exchange email
SharePoint sites
OneDrive accounts

Policy settings Edit

If the content has these types of sensitive information: France Social Security Number (INSEE),France Driver's License Number,France Passport Number,France National ID Card (CNI) then notify people with a policy tip and email message.

If there are at least 10 instances of the same type of sensitive information, block access to the content and send an incident report with a high severity level .

Turn policy on after it's created? Edit

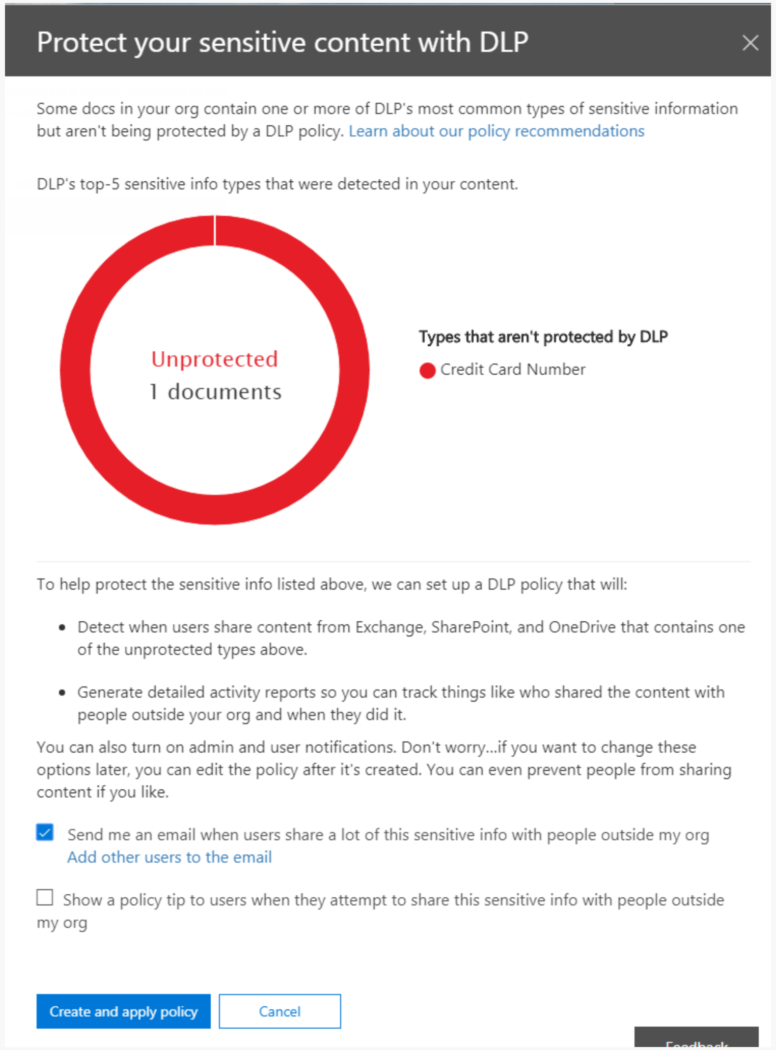
Test it out first. Don't apply actions or show policy tips to users.

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 of 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.

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

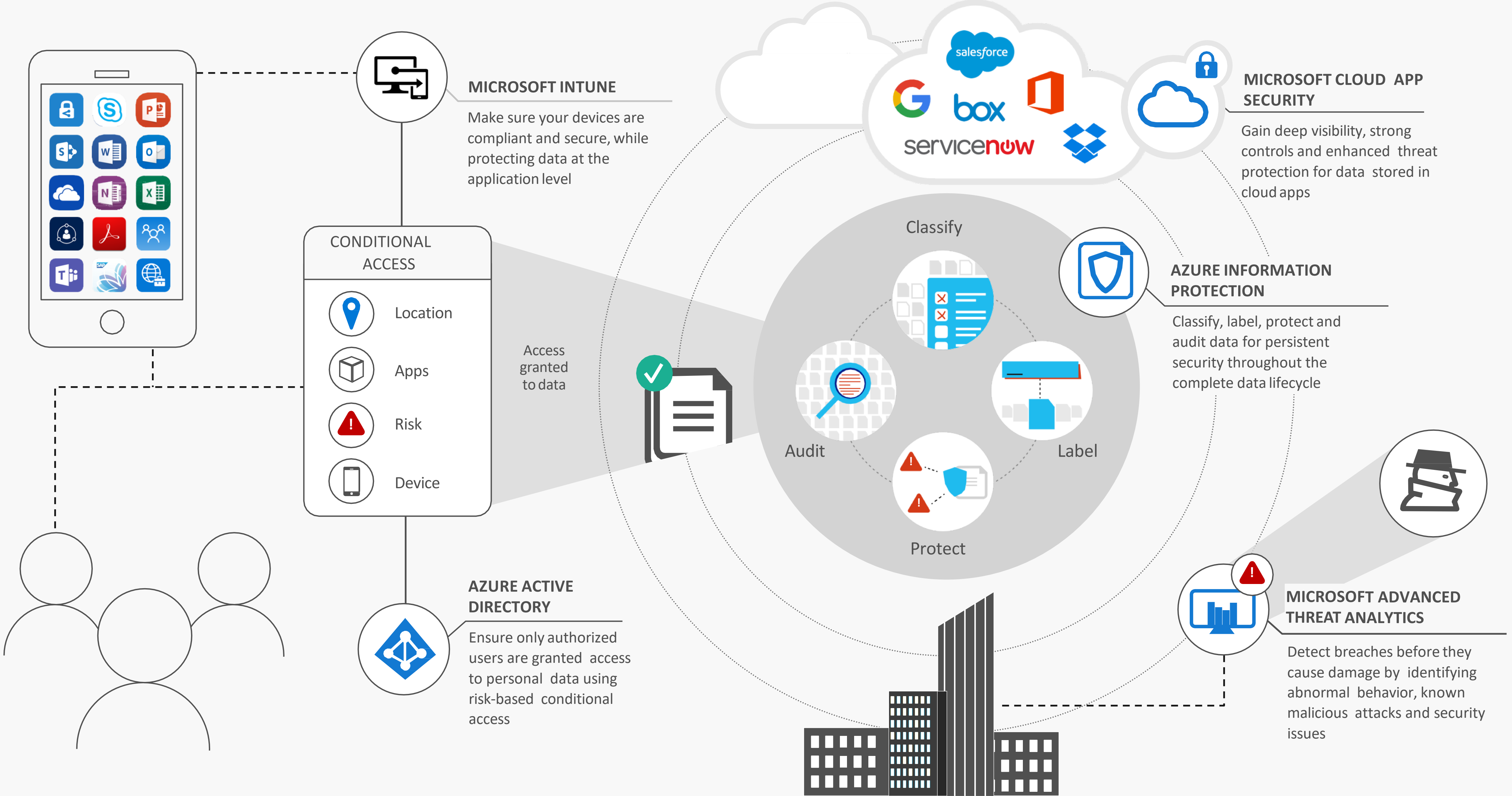
- Detect when users share content from Exchange, SharePoint, and OneDrive that contains one of the unprotected types above.
- Generate detailed activity reports so you can track things like who shared the content with people outside your org and when they did it.

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 lot 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

EMS – Protection layers



MICROSOFT INTUNE

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

CONDITIONAL ACCESS

- Location
- Apps
- Risk
- Device

Access granted to data

AZURE ACTIVE DIRECTORY

Ensure only authorized users are granted access to personal data using risk-based conditional access

MICROSOFT CLOUD APP SECURITY

Gain deep visibility, strong controls and enhanced threat protection for data stored in cloud apps

AZURE INFORMATION PROTECTION

Classify, label, protect and audit data for persistent security throughout the complete data lifecycle

Classify

Label

Protect

Audit

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

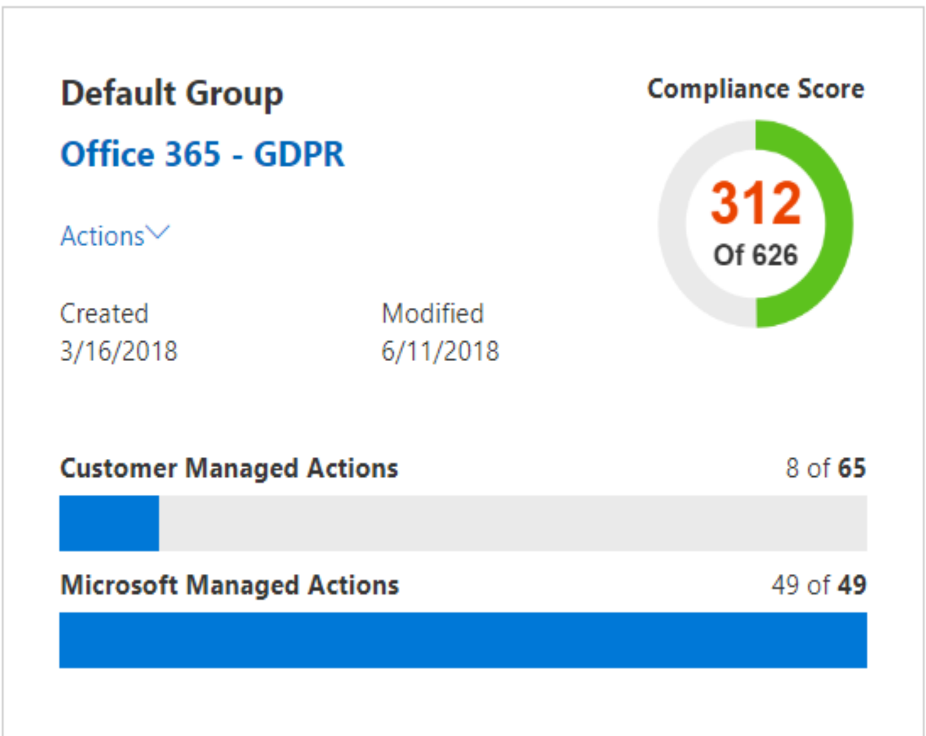
Dynamics 365
Reporting & Analytics

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



Default Group

Office 365 - GDPR

Actions

Created
3/16/2018

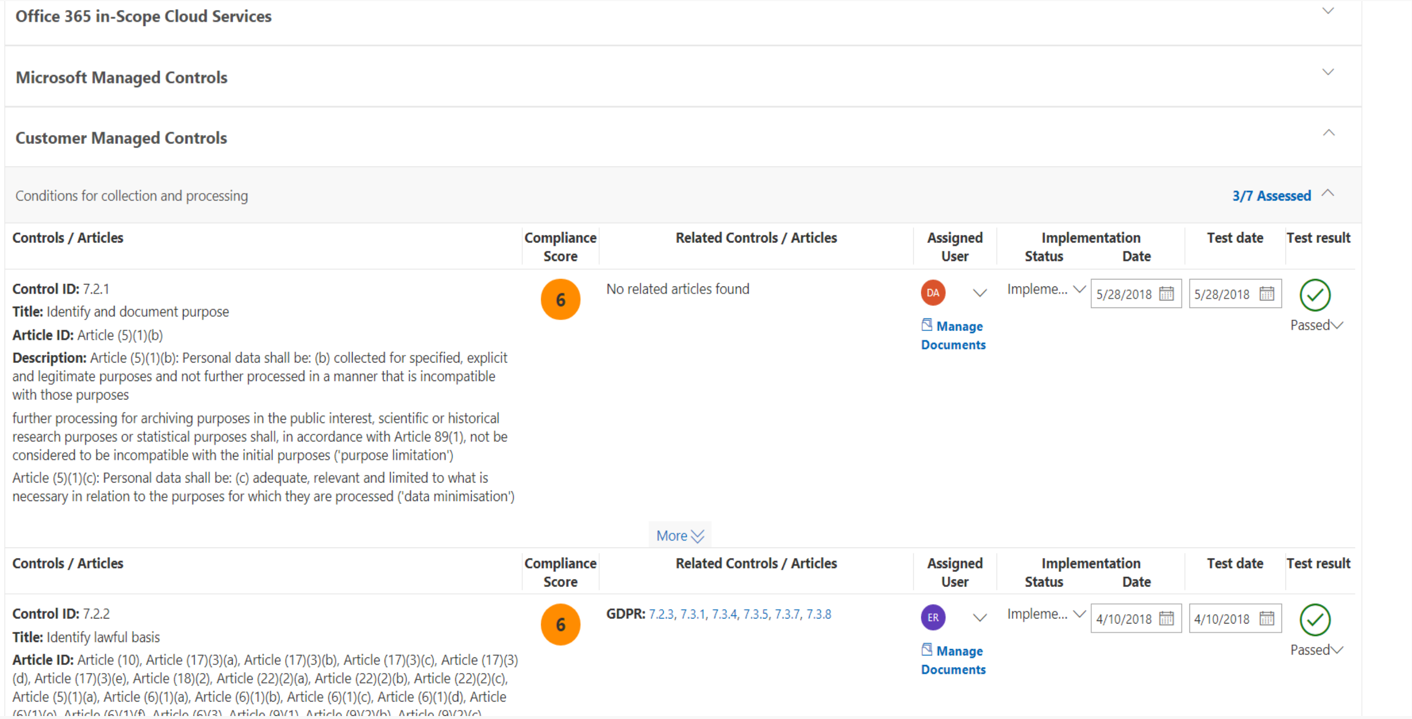
Modified
6/11/2018

Compliance Score

312
Of 626

Customer Managed Actions 8 of **65**

Microsoft Managed Actions 49 of **49**



Office 365 in-Scope Cloud Services

Microsoft Managed Controls

Customer Managed Controls

Conditions for collection and processing

3/7 Assessed

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation		Test date	Test result
				Status	Date		
Control ID: 7.2.1 **Title:** Identify and document purpose **Article ID:** Article (5)(1)(b) **Description:** Article (5)(1)(b): Personal data shall be: (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation') Article (5)(1)(c): Personal data shall be: (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')	6	No related articles found	DA Manage Documents	Impleme...	5/28/2018	5/28/2018	✓ Passed

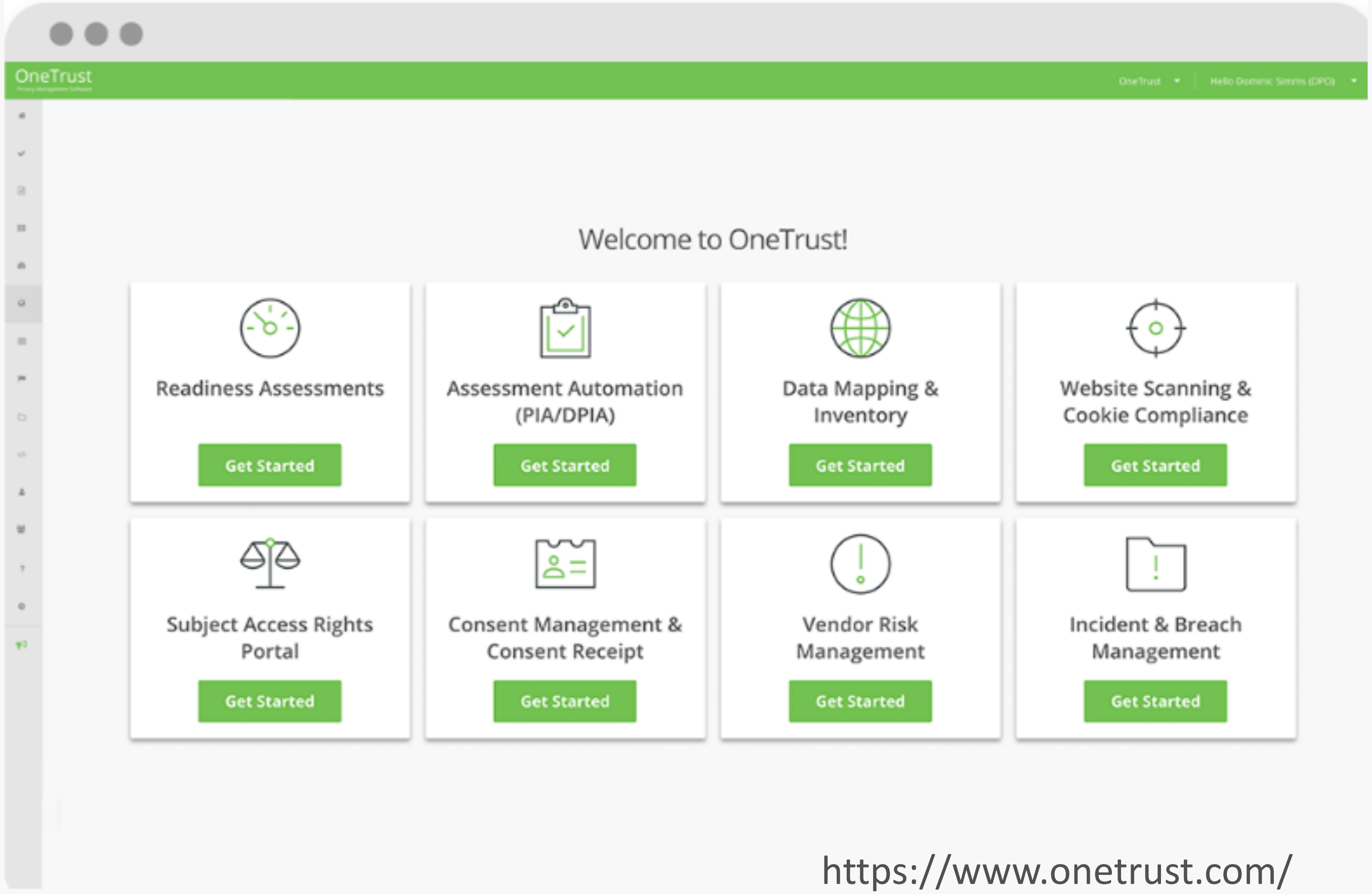
More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation		Test date	Test result
				Status	Date		
Control ID: 7.2.2 **Title:** Identify lawful basis **Article ID:** Article (10), Article (17)(3)(a), Article (17)(3)(b), Article (17)(3)(c), Article (17)(3)(d), Article (17)(3)(e), Article (18)(2), Article (22)(2)(a), Article (22)(2)(b), Article (22)(2)(c), Article (5)(1)(a), Article (6)(1)(a), Article (6)(1)(b), Article (6)(1)(c), Article (6)(1)(d), Article (6)(1)(e), Article (6)(1)(f), Article (6)(3), Article (9)(1), Article (9)(2)(b), Article (9)(2)(c)	6	**GDPR:** 7.2.3, 7.3.1, 7.3.4, 7.3.5, 7.3.7, 7.3.8	ER Manage Documents	Impleme...	4/10/2018	4/10/2018	✓ Passed

https://servicetrust.microsoft.com/ComplianceManager

GDPR Management Platforms

One Trust – Comprehensive platform

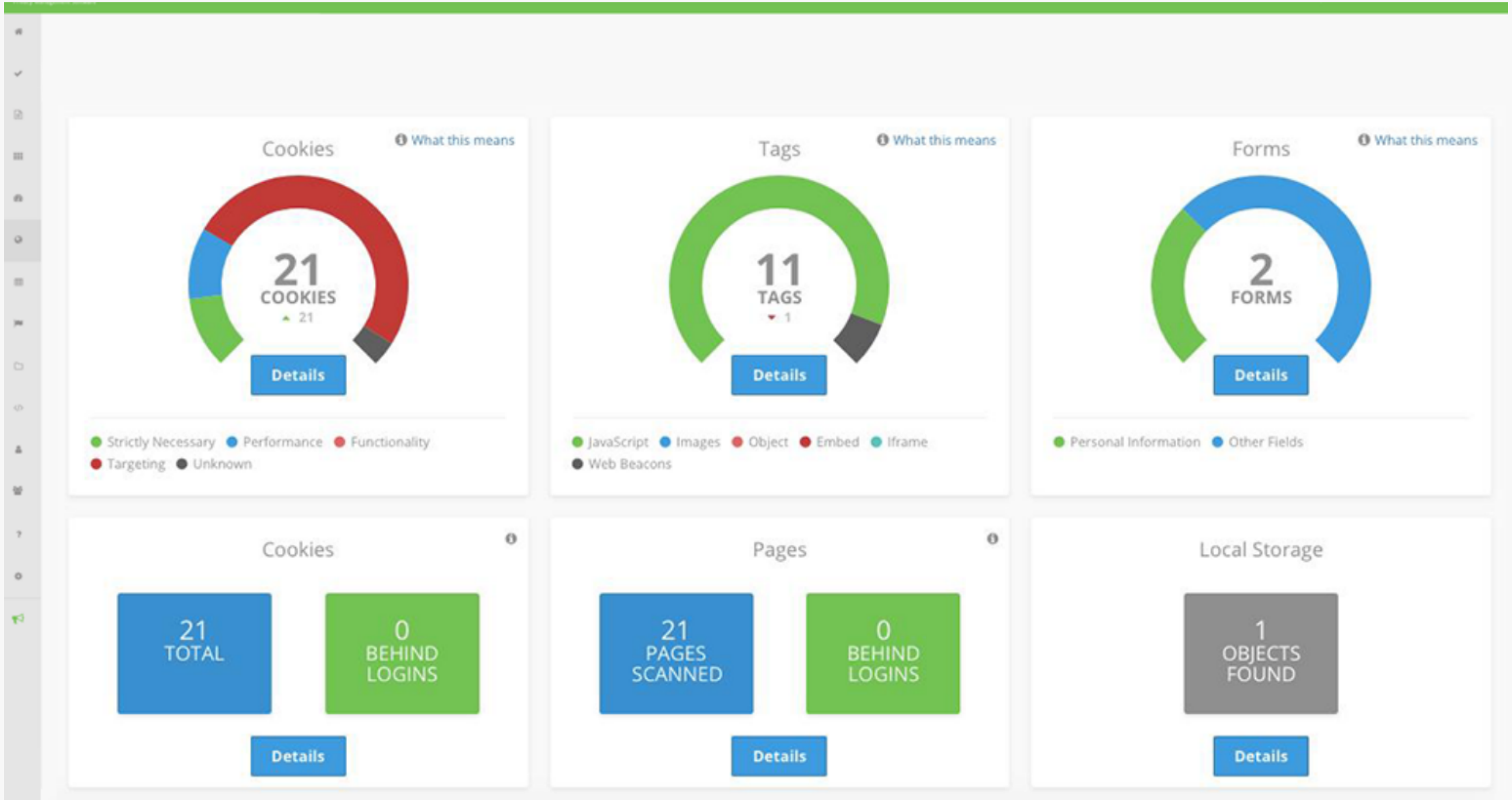


Welcome to OneTrust!

OneTrust
OneTrust
Hello Dominic Simms (DPO)
Readiness Assessments
Get Started
Assessment Automation (PIA/DPIA)
Get Started
Data Mapping & Inventory
Get Started
Website Scanning & Cookie Compliance
Get Started
Subject Access Rights Portal
Get Started
Consent Management & Consent Receipt
Get Started
Vendor Risk Management
Get Started
Incident & Breach Management
Get Started

https://www.onetrust.com/

One Trust – Risk Analytics



Cookies

21 COOKIES ▲ 21

● Strictly Necessary ● Performance ● Functionality ● Targeting ● Unknown

Tags

11 TAGS ▼ 1

● JavaScript ● Images ● Object ● Embed ● Iframe ● Web Beacons

Forms

2 FORMS

● Personal Information ● Other Fields

Cookies

21 TOTAL

0 BEHIND LOGINS

Pages

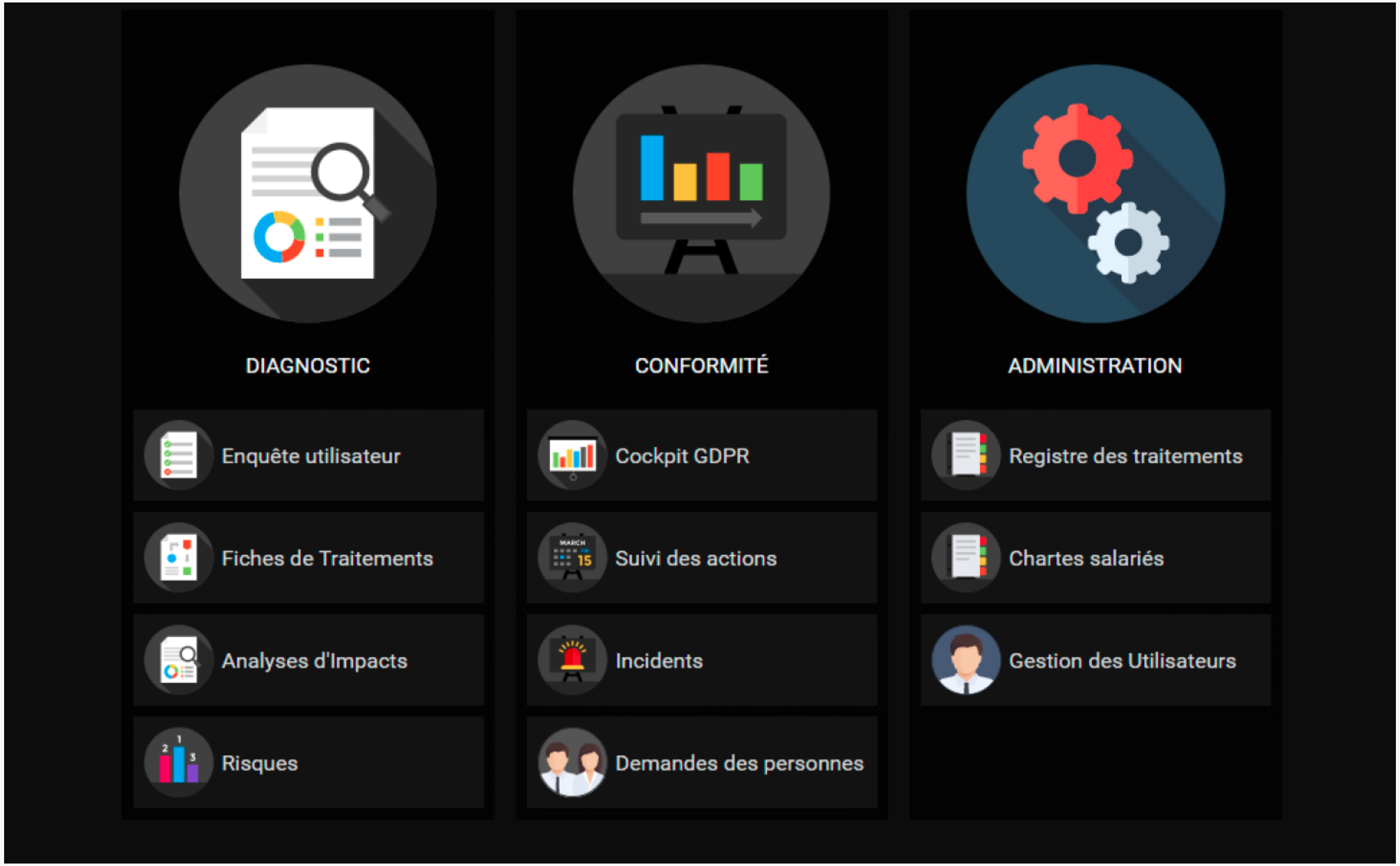
21 PAGES SCANNED

0 BEHIND LOGINS

Local Storage

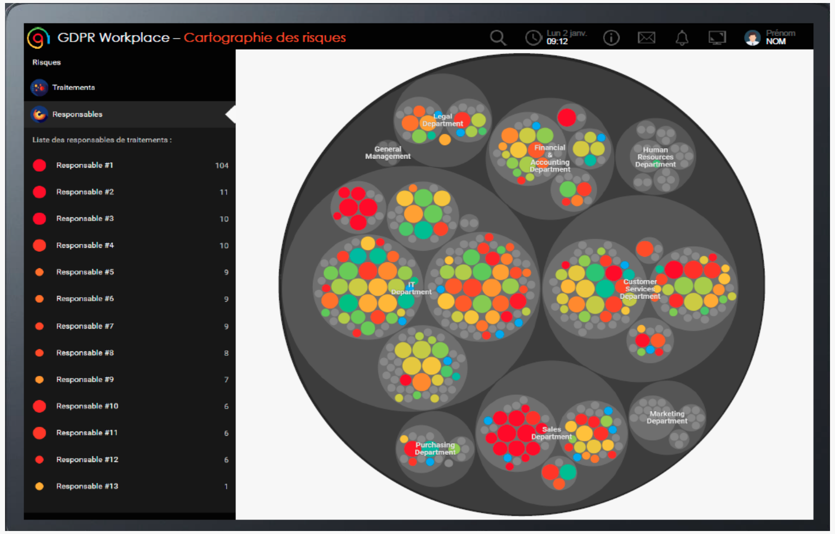
1 OBJECTS FOUND

GDPR Workspace



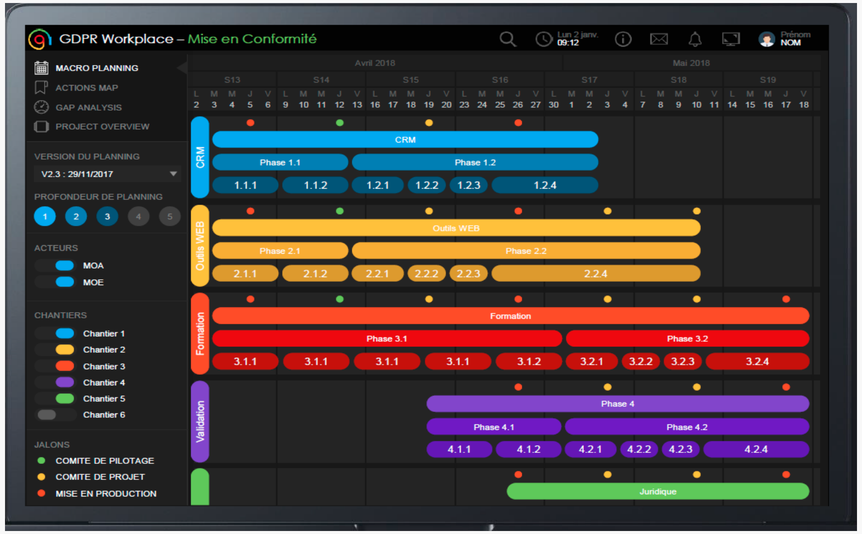
https://www.values-associates.com/fr/

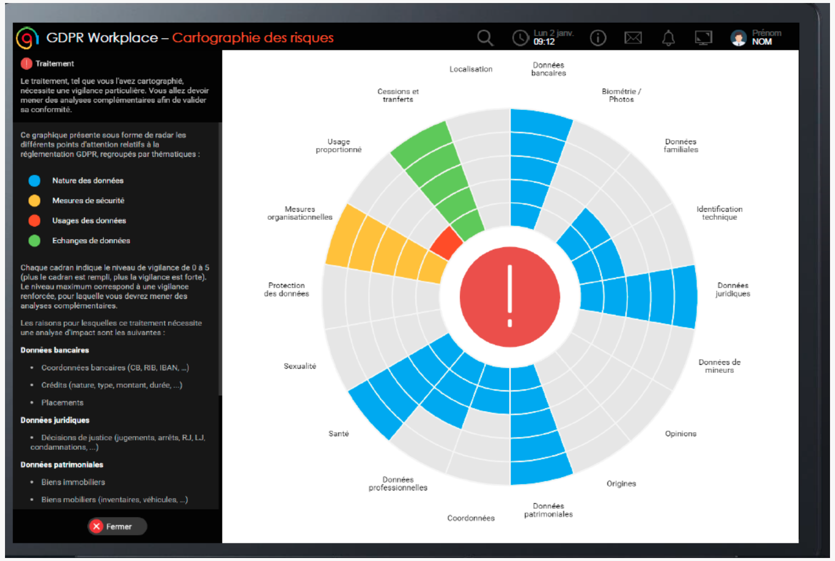
GDPR Workspace- Risks and remediation plans



Liste des responsables de traitements :

Responsable #1	104
Responsable #2	11
Responsable #3	10
Responsable #4	10
Responsable #5	9
Responsable #6	9
Responsable #7	9
Responsable #8	8
Responsable #9	7
Responsable #10	6
Responsable #11	6
Responsable #12	6
Responsable #13	1





Le traitement, tel que vous l'avez cartographié, nécessite une vigilance particulière. Vous allez devoir mener des analyses complémentaires afin de valider sa conformité.

Ce graphique présente sous forme de radar les différents points d'attention relatifs à la réglementation GDPR, regroupés par thématiques :

- Nature des données
- Mesures de sécurité
- Usages des données
- Echanges de données

Chaque cadran indique le niveau de vigilance de 0 à 5 (plus le cadran est rempli, plus la vigilance est forte). Le niveau maximum correspond à une vigilance renforcée, pour laquelle vous devrez mener des analyses complémentaires.

Les raisons pour lesquelles ce traitement nécessite une analyse d'impact sont les suivantes :

Données bancaires

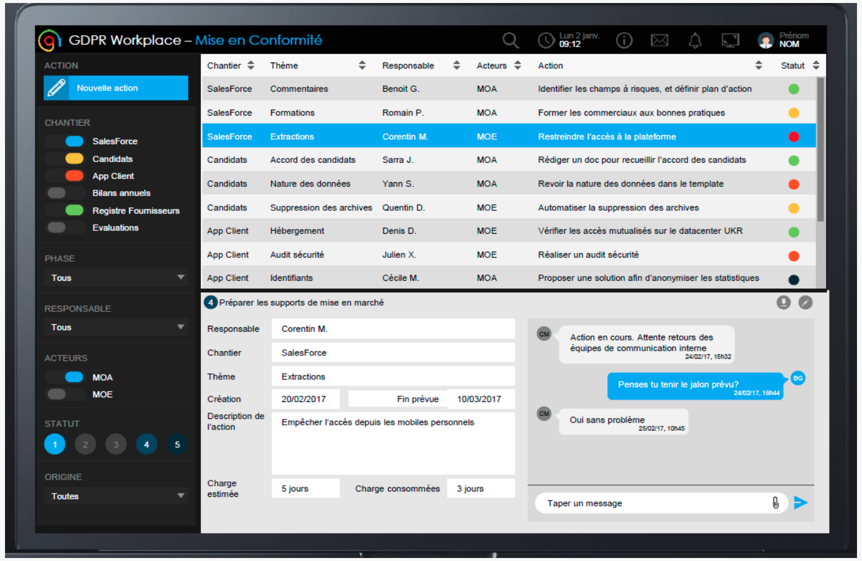
- Coordonnées bancaires (CB, RIB, IBAN, ...)
- Crédits (nature, type, montant, durée, ...)
- Placements

Données juridiques

- Décisions de justice (jugements, arrêts, RJ, LJ, condamnations, ...)

Données patrimoniales

- Biens immobiliers
- Biens mobiliers (inventaires, véhicules, ...)



Chantier	Thème	Responsable	Acteurs	Action	Statut
SalesForce	Commentaires	Benoit G.	MOA	Identifier les champs à risques, et définir plan d'action	●
SalesForce	Formations	Romain P.	MOA	Former les commerciaux aux bonnes pratiques	●
SalesForce	Extractions	Corentin M.	MOE	Restreindre l'accès à la plateforme	●
Candidats	Accord des candidats	Sarra J.	MOA	Rédiger un doc pour recueillir l'accord des candidats	●
Candidats	Nature des données	Yann S.	MOA	Revoir la nature des données dans le template	●
Candidats	Suppression des archives	Quentin D.	MOE	Automatiser la suppression des archives	●
App Client	Hébergement	Denis D.	MOE	Vérifier les accès mutualisés sur le datacenter UKR	●
App Client	Audit sécurité	Julien X.	MOE	Réaliser un audit sécurité	●
App Client	Identifiants	Cécile M.	MOA	Proposer une solution afin d'anonymiser les statistiques	●

4 Préparer les supports de mise en marché

Responsable: Corentin M.

Chantier: SalesForce

Thème: Extractions

Création: 20/02/2017 Fin prévue: 10/03/2017

Description de l'action: Empêcher l'accès depuis les mobiles personnels

Charge estimée: 5 jours Charge consommées: 3 jours

CM: Action en cours. Attente retours des équipes de communication interne 24/02/17, 15h32

BG: Penses tu tenir le jalon prévu? 24/02/17, 16h44

CM: Oui sans problème 25/02/17, 10h45

Taper un message

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