



NT KONFERENCA 2022

26. – 28. september 2022

#ntk22



Upravljanje s podatki v Microsoft 365

Slavko Kukrika

(Slavko.Kukrika@Outlook.com)

MCT in prijazen fant

Agenda

- ➔ Data classification
- ➔ Data Lifecycle and Records Management
- ➔ Information protection
- ➔ Data Loss Prevention
- ➔ Questions & Answers

Data Management in Microsoft 365

1

Understand what types of content you are storing

2

Classify so you can apply appropriate controls

3

Preserve information while you need it

4

Protect information based on sensitivity and risk

5

Dispose of information when no longer required

Data Classification

Know your data types!

All stored files are not equally important

Users can manually classify content (location, manual labeling ...)

We often prefer automatic classification

We can automatically classify content by using

- Sensitive info types

- Exact Data Match (EDM) classifiers

- Trainable classifiers

Sensitive Info Types

Commonly used method for classifying data

Identifies sensitive content through pattern matching

Microsoft 365 includes more than 300 built-in sensitive info types

Many are country or region specific (Passport number, Driver's license number, ...)

Copy built-in info type to see how it is built

Create new Sensitive info type by using following primary element:

Regular expression

Keyword list

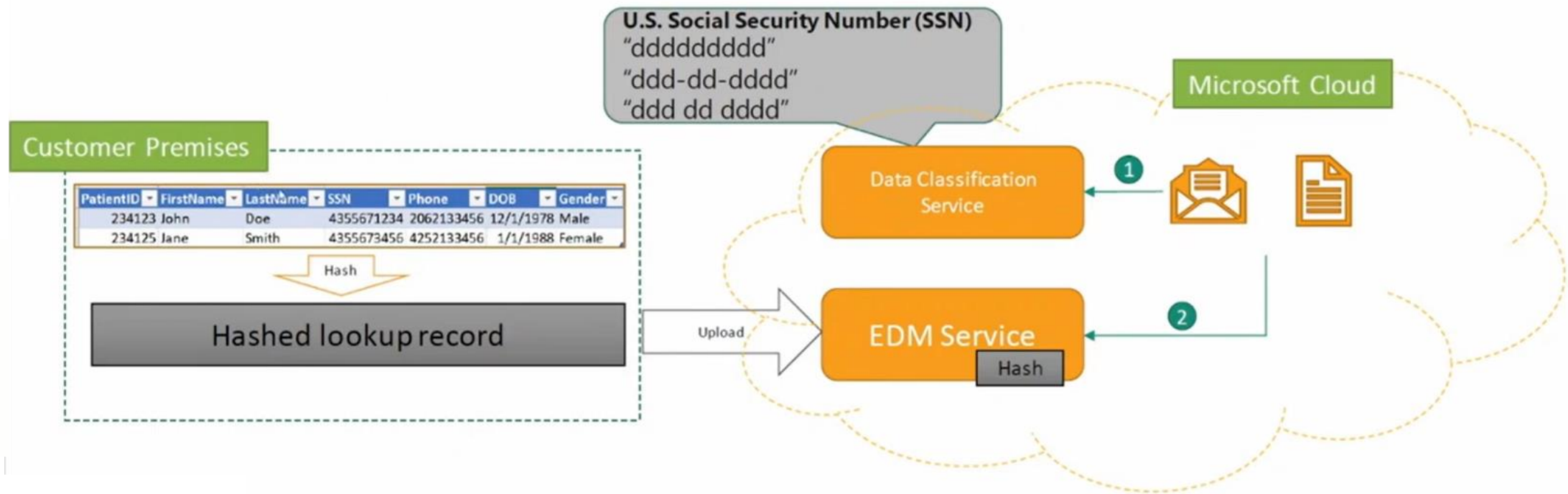
Keyword dictionary

Function

Name ↑	
<input type="checkbox"/>	Slovenia Driver's License Number
<input type="checkbox"/>	Slovenia Passport Number
<input type="checkbox"/>	Slovenia Physical Addresses
<input type="checkbox"/>	Slovenia Tax Identification Number
<input type="checkbox"/>	Slovenia Unique Master Citizen Number

Exact Data Match (EDM)

Use exact values to detect matches instead of generic patterns



Trainable classifiers

Sensitive info types are good for matching specific patterns in data

Trainable classifiers use a machine learning to classify less predictable formats

There are two types of trainable classifiers:

- Pre-Trained Classifiers








- Custom Trainable Classifiers

Can be used with:

- Retention auto-labeling policies

- Sensitivity auto-labeling policies

- Communication compliance

▼ Published (50)			
<input type="checkbox"/>	Agreements		-
<input type="checkbox"/>	Customer Complaints(preview)		-
<input type="checkbox"/>	Discrimination		-
<input type="checkbox"/>	Finance		-
<input type="checkbox"/>	HR		-
<input type="checkbox"/>	Healthcare		-
<input type="checkbox"/>	IP		-

NT KONFE RENCIA 2022

Demo

Creating Sensitive info type
Exploring Trainable classifiers

Data Lifecycle and Records Management

Labels control how data (files) are managed

Assignment can be manual (publish, inherit) or automatic (auto-apply)

Files can be assigned a retention period

Retention period can start at different events (when created, modified, labeled or event based)

During retention period files cannot be removed

At the end of retention period they can have disposition review

Documents may become immutable: while a Record, we cannot modify, edit or delete a document

Regulatory record is even more restrictive (cannot be removed, can only extend retention)

Data Lifecycle Management



Retention Labels

Create a unified label to manage retention, deletion and disposition reviews at a granular level.

Use for documents & emails.



Retention Label Policies

Publish retention labels to locations throughout Microsoft 365.

Publish to Exchange mailboxes, SharePoint Sites, OneDrive accounts, Microsoft 365 Groups



Retention Policies

Manage retention and deletion.

Use for Microsoft Teams Chat & Channel Messages, Skype for Business, Exchange Public Folders Content

Use also for Exchange Mailboxes, SharePoint sites, OneDrive accounts, Microsoft 365 Groups

Retention Labels and Retention Label Policies

Retention Labels

Define our record types, including retention periods, disposition actions, etc.



Budgets

ID: 0100

Retention: 5 years,
Trigger: Fiscal Year End,
Final Disposition: Destroy



Contracts (Master Set)

ID: 0110

Retention: 10 years
Trigger: Contract Expiry & Full Satisfaction of conditions
Final Disposition: Destroy



Financial Reports– General Ledgers

ID: 0120

Retention: 10 years
Trigger: Fiscal Year End
Final Disposition: Destroy



Retention Label Policies

Publish Retention Labels to sites, mailboxes, etc. by using Retention Label Policies



Publish Budgets & Contracts



Publish Contracts



Publish Contracts & Financial Reports



Financial Reports – General Ledger

Locations

The locations where we store and work with content

(all) Exchange mailboxes
(3) SharePoint sites
(10) OneDrive accounts
(3) Microsoft 365 groups

(0) Exchange mailboxes
(1) SharePoint sites
(0) OneDrive accounts
(1) Microsoft 365 groups

(0) Exchange mailboxes
(1) SharePoint sites
(0) OneDrive accounts
(1) Microsoft 365 groups

(7) Exchange mailboxes
(1) SharePoint sites
(0) OneDrive accounts
(0) Microsoft 365 groups

Retention label and Retention policy locations

- A **retention policy** is published to a location and applies to all content within the location



1:1 and Group chats
Standard Channel msgs
Private Channel msgs



Community msgs
Private msgs



- A **retention label policy** is published or auto-applied to specific **items** within the location



Published: Retention label will be visible to end-users in the UI allowing them to apply it to an item



Auto-applied: Retention label will be automatically applied to an item based on conditions you supply

Comparing Retention Labels and Retention Policies


	Retention Labels	Retention Policies
Apply Retention	X	X
Event Based Retention	X	
Manage SharePoint, OneDrive, Groups, Exchange Email Content	X	X
Manage Microsoft Teams Conversations, Skype for Business Chat, Exchange Public Folders Content		X
Manage Content as a [finalized] Record	X	
Apply Based on Sensitive Information	X	
Apply Based on Specific Words and Phrases	X	
Granularity to specific documents or emails	X	

Automatically apply Retention Labels



SharePoint Library Default Label

-  Auto-applied to documents when added to a document library
-  Can apply to existing documents in the library

Retention Label on a Folder

-  Apply a retention label to a folder to apply to all documents in the folder

Auto-Apply Policies

-  Auto-applied based on sensitive information types
Exchange (all mailboxes only), SharePoint, OneDrive
-  Auto-applied based on a search query or a trainable classifier
Exchange, SharePoint, OneDrive, Office 365 groups

Apply Retention Labels with Auto-Apply Policies



NT KONFERENCA 2022

Demo

Creating and publishing
Retention label
Applying Retention label

Microsoft Information Protection

Create Sensitivity label

- Content marking
- Encrypting content
- Rights management

Publish Sensitivity label (apply manually)

- Publish to users and groups

Set default sensitivity label for a library

Auto-labeling

- Exchange, SharePoint, OneDrive
- Conditions include Sensitive info types and trainable classifiers (are workload specific)



Applying Sensitivity Labels Automatically

Client-side labelling

- Classifies based on sensitive info types (pattern matching)
- Works in Office client apps (Outlook, Word, Excel, PowerPoint)
- Apply label automatically
- Recommend that the user applies a label

Service-side labelling

- Classifies based on sensitive info types (pattern matching)
- Data at rest (documents stored in SharePoint and OneDrive)
- Data in transit (emails sent or received by Exchange)
- Labelling at scale

Data Loss Prevention (DLP)

Prevent inappropriate sharing of sensitive data

Scope

Where to apply DLP policy

Conditions

To which content to apply DLP

Actions

Which actions to take

Endpoint DLP

Windows and macOS devices, onboarded to Microsoft Purview



NT KONFERENCA 2022

Demo

Creating DLP policy

Viewing DLP protected content

Summary

Microsoft Purview Compliance portal is used for data management

Classify data first

Use Sensitivity labels to protect data (documents)

Use DLP policies to prevent accidental sharing of sensitive information

Use Retention labels to manage data lifecycle

Additional information

Learn about sensitive information types

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-learn-about>

Protect your sensitive data with Microsoft Purview

<https://learn.microsoft.com/en-us/microsoft-365/compliance/information-protection>

Learn about data loss prevention

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp>

Learn about retention policies and retention labels

<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention>

Flowchart to determine retention or deletion

<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention-flowchart>

Questions?

Slavko.Kukrika@Outlook.com



This is not school, but we **love** to get grades. Please fill out our questoineers and leave us your feedback. You may even **win** some cool rewards.

NT KONFE RENCA 2022

PORTOROŽ

26. – 28. september 2022