Compliance in Office 365

Guhan Ramasamy

Cloud Solution Architect

guhan.ramasamy@capgemini.com

Need for Compliance:

In current digital world, organization handles an enormous amount of data which lead to the risk of sensitive data exposed to people who are not supposed to access the information. Storing and performing the data operation through the cloud-based solution many folds increase the risk of exposing sensitive data to the rest of the world.

All the countries and organizations around the globe having a concern about exposing sensitive data to unauthorized people to address this risk various authorities have come up with Country and domain specific compliance. GDPR, PII and HIPPA are few of the compliance related to specific region and domain.

One of the largest hotel chains fined around euro 100 Million by GDPR council for exposing the sensitive data and not compliance with GDPR. This shows how important it is to handle the data in a very secure way.

It has become necessary for all organizations around the world to implement country and domain specific compliance in order to perform their business effectively.

This article will provide the knowledge about how to implement compliance in **Office365** content.

Compliance in Office365:

Microsoft as a leading ISV and world's largest office productivity software provider handles sensitive data by implementing the standardized country and domain-specific solution in Office365 and provides a provision to create custom organization-specific compliance.

Office365 added **"Security and Compliance" portlet to** Implement, Monitor and Identify Incident with action to be taken.

Office365 provided the option of **classification** of sensitive data by means of **labels** and **DLP (Data Loss Prevention) policies.** Labels can be **manually** or **automatically** applied to the office 365 suite.

Office365 Labels:

Labels are easy to understand **tags** which are created by office365 admin by collaborating with compliance manager which can be applied across organization and office 365 suite. Labels, in turn, provide the definition/rule to classify the office 365 artifacts.

For example, organization can classify the artifacts as High, Medium and Low sensitive data based on the label definition which are set while creating the label.

There are two types of labels available in Office365 to apply compliance

- Sensitive Label
- Retention Label

Sensitive Label:

Sensitive labels help organizations classify the office 365 artifacts based on their sensitivity of the information that is presented in the artifact. By labeling procedure sensitive label further classified into the below listed item.

- Manual Label
- Auto Label

Manual Label:

In this process user manually classifies and tags the artifact by reading and understanding the sensitivity of the content.

Auto Label:

Auto Label feature is only available only in the **Office365 E5** Plan. This feature makes our life easier by applying the labels automatically to the Office365 artifacts based on the pre-defined compliance rule including key compliance like **GDPR, SOX, PCII,** etc. This predefined compliance in Office 365 is called as **"Sensitive Info Type".**

Sensitive Info Type:

Sensitive info type is the **pre-definition rules** which help to identify the artifacts having **sensitive information**. Sensitive info type is the key component that allows organizations to apply **country, domain and organization** specific compliance to the organization content. To ease our life, Microsoft provides around **100+ ready to apply pre-defined industry and domain standard compliance** that can be applied to **Office365** artifacts as required.

Retention Label:

Retention labels are the special type of labels that provide the definition for classification with information on how long Office365 artifacts are to be retained.

Using this label after retention period we can set the option to auto delete the artifact, Trigger workflow for review and declare the artifact as record.

Label Policy:

Label Policy plays a key role in compliance where it will dictate what action to be taken in labeled component. Label policy applies to **"Sensitive Label"** and **"Retention Label".**

Label policy will have the definition to whom the labels to be applied and what is the process and actions to be followed.

It is **mandatory** for each label to have a label policy. Without a label policy respective label can't be accessed by users.

Data Loss Prevention (DLP):

The mechanism or **procedure** to prevent data loss and data leakage of organization specific information is called **data loss prevention (DLP).** If any organization has not implemented DLP, they are at a very high risk of leakage and loss of data in the digital world may lead to large financial liability, spoil the company reputation in the market and finally legal issues.

Data Leakage:

Accidental or **Intentional sharing** of data with other individuals or organizations which are classified as sensitive data may lead to the data leakage.

For example, user of "Organization A" shares the contract related information with a competitor organization is considered as a data leakage.

Data Lost:

Accidental or Intentional **deletion/removal/loss** of data which should be retained and maintained as per compliance/rules. Data Loss may lead to data leakage where deleted/removed/lost data reaches the custody of unwanted people/organization.

For example, user of "Organization A" shares contract related information with the competitor and also permanently deletes/removes the contract details from "Organization A" is called as data lost.

Need for DLP Product:

Even though we are having network level security to granular field level encryption in a software product to protect our data due to the evaluation of Internet, Cloud Computing and Artificial Intelligence, risk of data leakage and data loss is still very high.

Recent leakage of a county specific sensitive government information to the public knowledge base WikiLeaks spoiled the reputation of the government and relationship with other countries is a classic example to understand how important to protect the sensitive information.

EMC DLP, McAfee DLP, CA DLP are the leading DLP products in the market which protect the **data in rest** and **in motion** in context of **cloud** and **on-premise.**

Microsoft Offering of DLP:

Microsoft provides DLP protection to the data stored in **Windows servers, Windows client** and their public cloud offerings **Azure** and **Office365** with **Windows Information Protection (WIP), Microsoft Intune, Azure Information Protection (AIP) and Office365 security and compliance center.**

DLP in Office365:

In office365, DLP implemented across all the office365 products through Office365 security and compliance center. In Office365, DLP is implemented in the form of **policy.** Once DLP policy created policy can be applied to the needed office365 products.

Data Loss Prevention Policy (DLP):

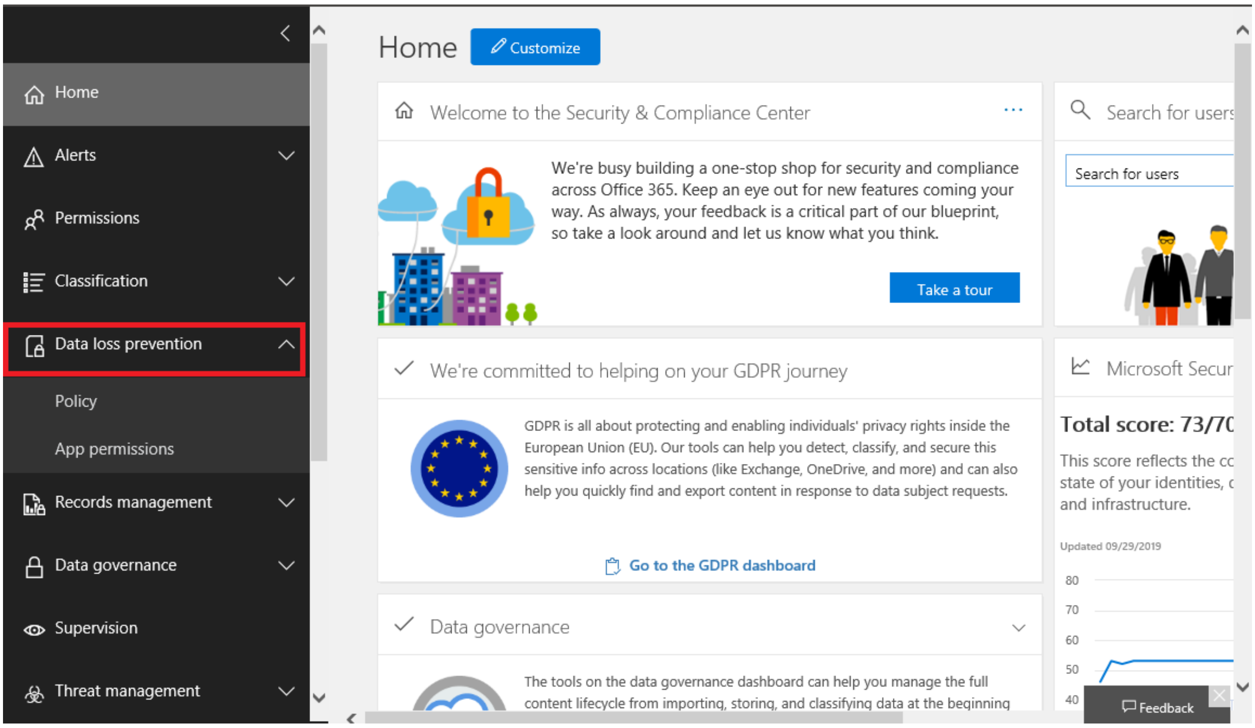
Data Loss prevention policy is a great tool to protect the financial data or personally identifiable information (PII) across the compliance boundary. DLP policy helps to identify the sensitive information across Office365 landscape and provides the actions to be taken. **DLP Dashboard** and **interactive reports** will help **compliance officers** to monitor the **compliance breach** and take necessary actions.

Applying DLP will provide peace of mind to the organization where it has the business need to share the information within the organization and **outside** the organization. Through DLP, we can set the rules to **prevent** information which are classified **sensitive** to cross the organization boundary.

One of the major benefits of DLP policy is that it can be pushed to the offline apps like **MS Office** and **MS Exchange** client.

How to create and apply DLP Policy:

DLP Policy can be created by the **Compliance manager** by simply logging in to the office365 **"Security and Compliance Center".**



We're busy building a one-stop shop for security and compliance across Office 365. Keep an eye out for new features coming your way. As always, your feedback is a critical part of our blueprint, so take a look around and let us know what you think.

GDPR is all about protecting and enabling individuals' privacy rights inside the European Union (EU). Our tools can help you detect, classify, and secure this sensitive info across locations (like Exchange, OneDrive, and more) and can also help you quickly find and export content in response to data subject requests.

Total score: 73/70

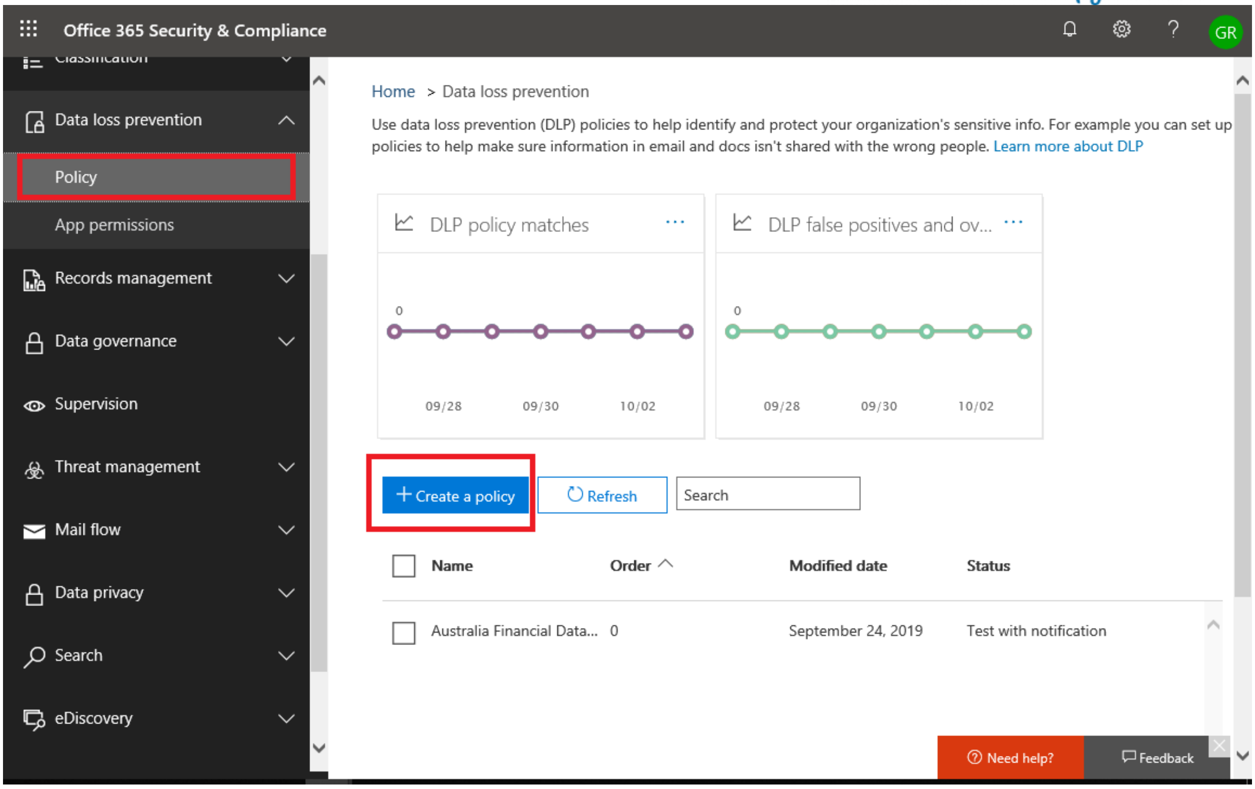
This score reflects the co state of your identities, d and infrastructure.

The tools on the data governance dashboard can help you manage the full content lifecycle from importing, storing, and classifying data at the beginning

What is DLP Policy:

DLP policy provides **definition/rules** about the sensitive information, to **whom & which** Office365 product policy to be applied and finally what actions are to be taken on an artifact that have been tagged as sensitive information.

Please refer below screenshot to create DLP Policy



Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP

☐	Name	Order	Modified date	Status
☐	Australia Financial Data...	0	September 24, 2019	Test with notification

Policy rule with DLP:

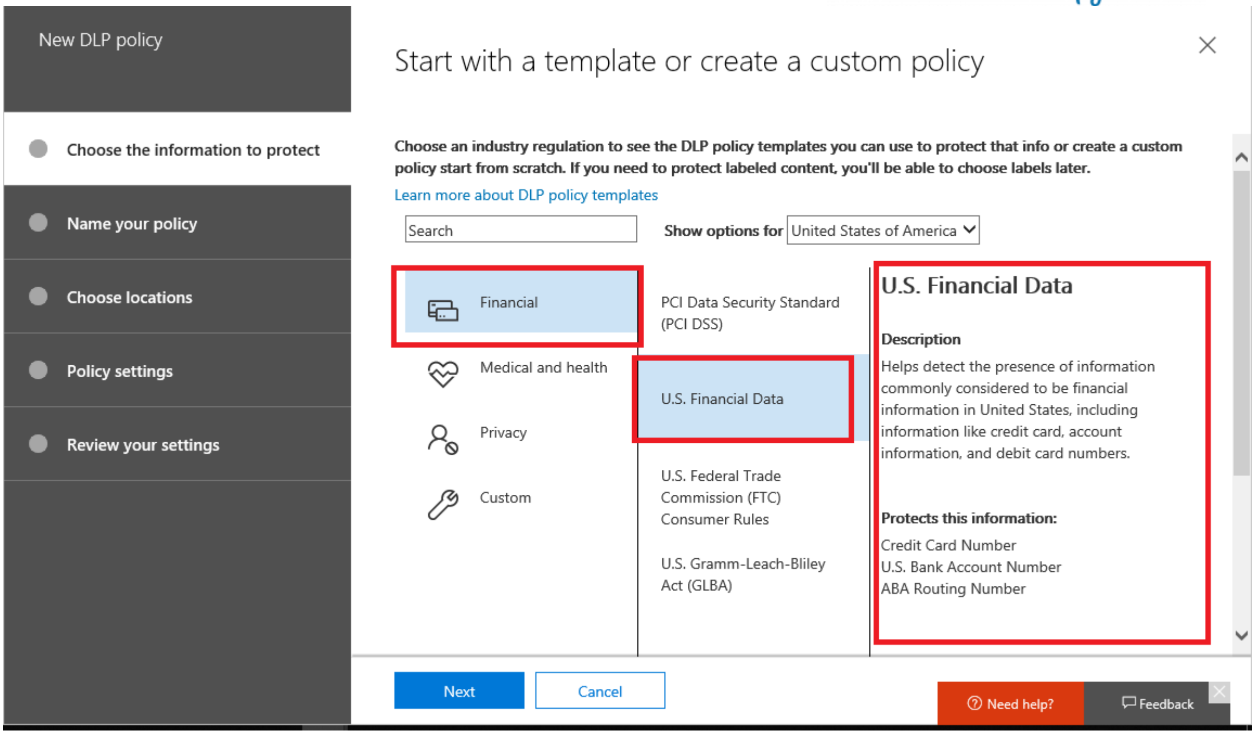
Policy rules dictate the definition of sensitive data. With this definition, Office365 will identify the sensitive artifacts.

Microsoft provides all together around **100+** country specific and domain specific **pre-defined** policy rules that help compliance manager to implement the policy in a very quick turnaround time without any help from the IT team.

Office365 security center also provides the option to create custom sensitive data rules.   This option can be used to create organization specific policy definition from scratch or from the pre-defined policy definition.

Whenever a new country or domain specific compliance gets published, Microsoft usually add the **definition/rules** immediately in Office365.This reduces the need for creating custom rules in real-time scenario.

Below screenshot shows the pre-defined **U.S Financial Data definition**



New DLP policy

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

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later.

Learn more about DLP policy templates

Search | Show options for: United States of America

Financial	PCI Data Security Standard (PCI DSS)	U.S. Financial Data
Medical and health	U.S. Financial Data	
Privacy	U.S. Federal Trade Commission (FTC) Consumer Rules	
Custom	U.S. Gramm-Leach-Bliley Act (GLBA)	

U.S. Financial Data

Description

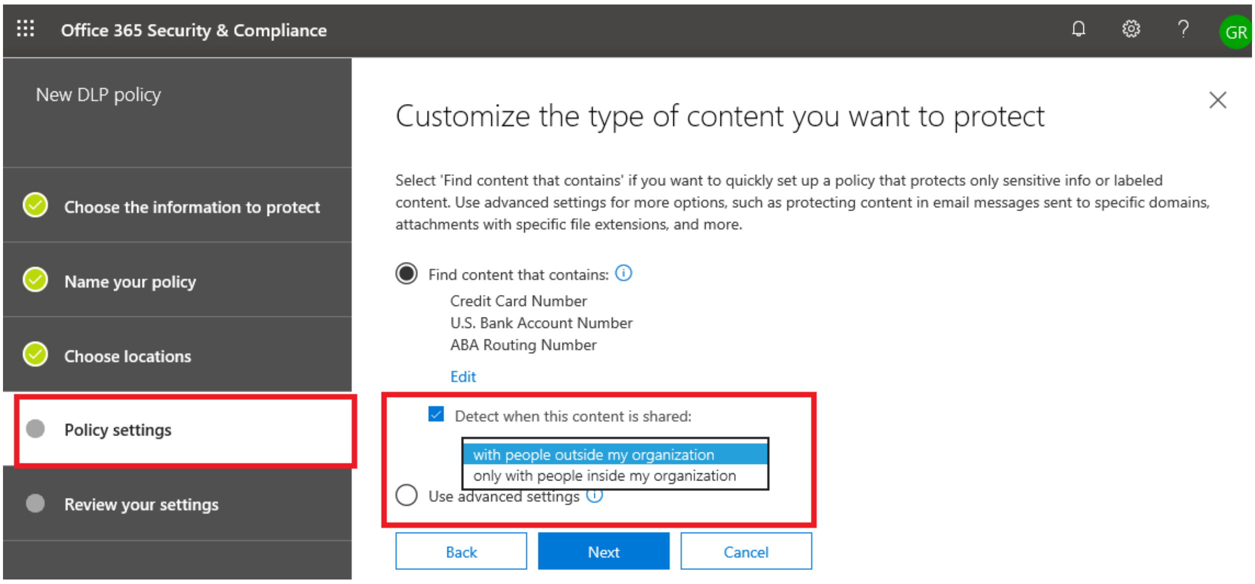
Helps detect the presence of information commonly considered to be financial information in United States, including information like credit card, account information, and debit card numbers.

Protects this information:

Credit Card Number
U.S. Bank Account Number
ABA Routing Number

By using Office365 policy we can protect all office365 artifacts. Office365 provides the option to select whether we must protect all the office365 artifacts or specific type of office365 artifacts using the DLP policy.

Through **"Policy settings"** option, compliance manager can provide the option to choose whether the policy has to be applied for users **within the organization or outside the organization.**



New DLP policy

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

Customize the type of content you want to protect

Select 'Find content that contains' if you want to quickly set up a policy that protects only sensitive info or labeled content. Use advanced settings for more options, such as protecting content in email messages sent to specific domains, attachments with specific file extensions, and more.

● Find content that contains:
Credit Card Number
U.S. Bank Account Number
ABA Routing Number
Edit

☑ Detect when this content is shared:
with people outside my organization
only with people inside my organization

○ Use advanced settings

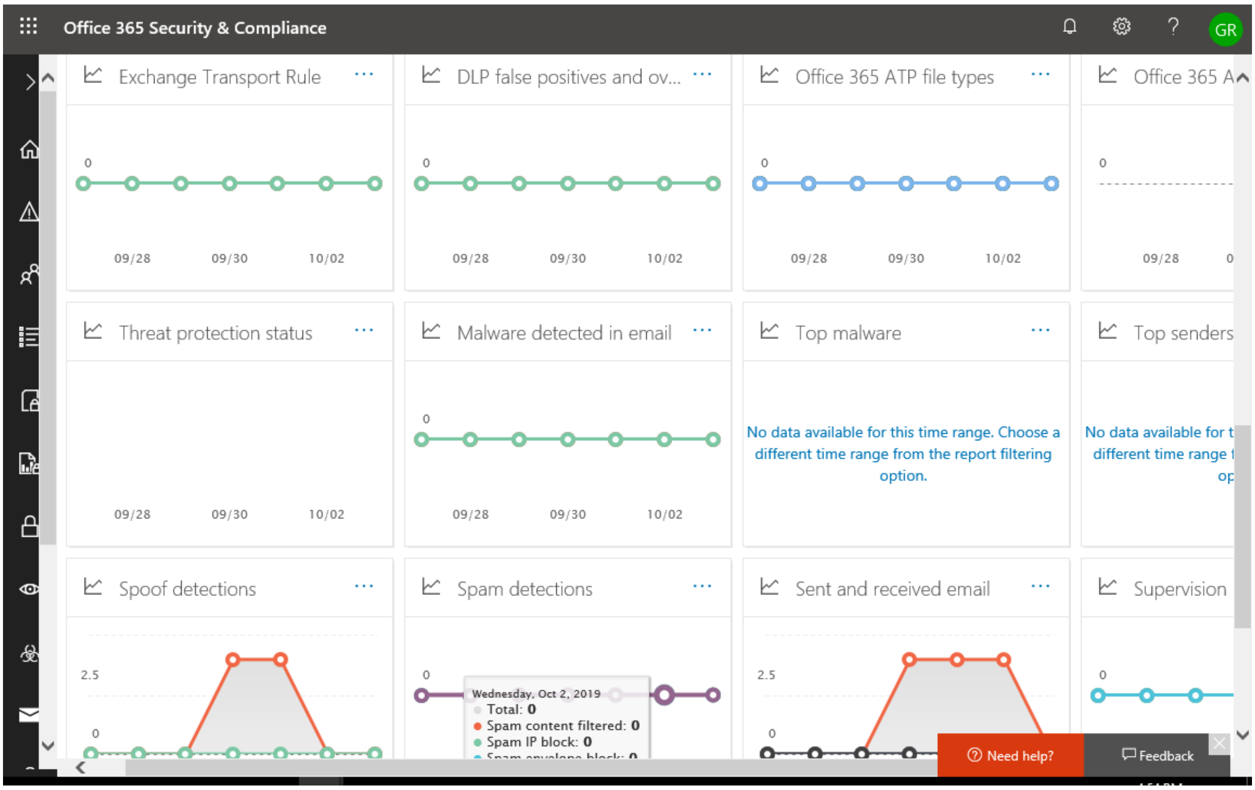
Through **"Advance settings"** of the **"Policy Settings"** compliance manager can provide with the option to modify **pre-defined rules** and provides option to add addition rules with priority.

Dashboard in Security and Compliance Center:

Office365 Security and Compliance center provides interactive dashboard to monitor security breach across the Office365 product suite with **periodic** and **ad-hoc** reporting capability.   Also, Microsoft provides the option to create a **custom** dashboard and **custom** reports based on the organization's needs.

All the security breaches and incidents are monitored and reported **real time** to compliance managers through dashboard and reports to take quick needed actions.

Below screenshot provide a view of built-in dashboard



No data available for this time range. Choose a different time range from the report filtering option.

No data available for t different time range f op

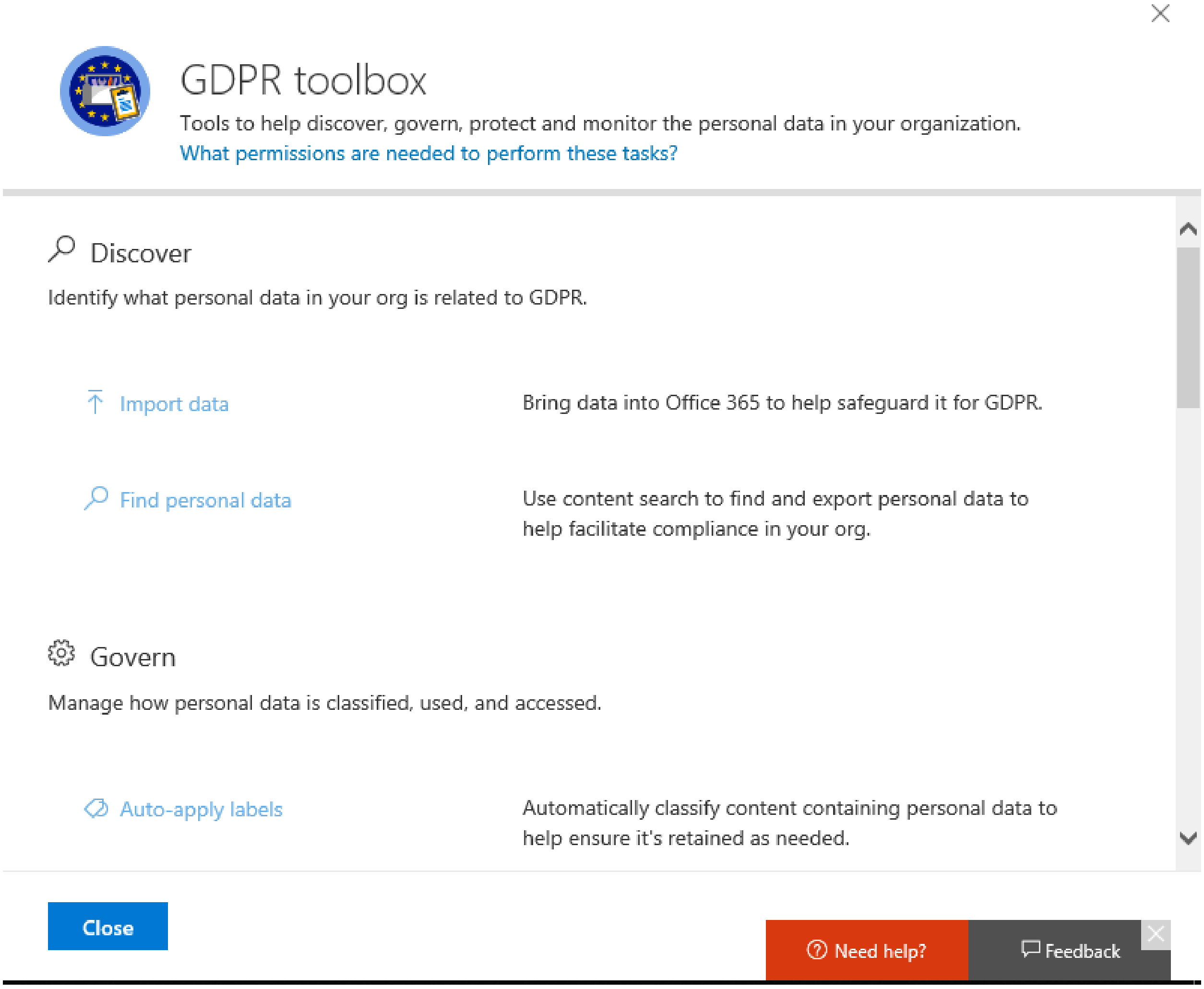
Wednesday, Oct 2, 2019
Total: 0
Spam content filtered: 0
Spam IP block: 0
Spam envelope block: 0

GDPR Implementation in Office365:

Office365 implements GDPR by using **auto labels, retention labels,** and **DLP Policy.** There is a separate section and separate **built-in dashboard** available in the "Security and compliance Center" of Office365.

Office365 provides a separate toolbox named **"GDPR Toolbox"** to implement and handle **GDPR compliance**. This toolbox helps **compliance manager** and **Office365 Admin** to discover the data for GDPR compliance by using Office365 search feature followed by defining the **rules** to classify the discovered data and finally it provides the option of what actions need to be taken on **discovered and classified** GDPR **non-compliance** data.

Below Image provide the snapshot of GDPR Toolbox



GDPR toolbox

Tools to help discover, govern, protect and monitor the personal data in your organization.

What permissions are needed to perform these tasks?

Discover

Identify what personal data in your org is related to GDPR.

Import data	Bring data into Office 365 to help safeguard it for GDPR.
Find personal data	Use content search to find and export personal data to help facilitate compliance in your org.

Govern

Manage how personal data is classified, used, and accessed.

Auto-apply labels	Automatically classify content containing personal data to help ensure it's retained as needed.

Conclusion:

Office365 as a leader of the Content & Collaboration segment fulfils the need for compliance requirement of the organization using "Security and Compliance Center". In Office365, we can implement around 100+ country and domain specific compliance solutions in quick turnaround time by using in-built ready to use compliance rules/definitions. Also, office365 provides an option to create custom organization and country specific rules/definitions.

In summary, through Office365 "Security and Compliance Center" we can identify, monitor and take appropriate action on the data which are not adhered to compliance.

About Sogeti

Sogeti is a leading provider of technology and engineering services. Sogeti delivers solutions that enable digital transformation and offers cutting-edge expertise in Cloud, Cybersecurity, Digital Manufacturing, Digital Assurance & Testing, and emerging technologies. Sogeti combines agility and speed of implementation with strong technology supplier partnerships, world class methodologies and its global delivery model, Rightshore®. Sogeti brings together more than 25,000 professionals in 15 countries, based in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Capgemini SE, listed on the Paris Stock Exchange.

Learn more about us at

www.sogeti.com