



**MAKE IT**  
**cLOUD**

Neum 18-20/4/2018

NetWork 

Pripremite se za Uredbu o zaštiti podataka EU (GDPR) sa  
Microsoft servisima i Office 365

Tomislav Lulić

ECS – Eurocomputer Systems, Zagreb







# Pripremite se za Uredbu o zaštiti podataka EU (GDPR) sa Microsoft servisima i Office 365

Tomislav Lulić  
ECS – Eurocomputer Systems



 Office 365





platinum sponsor

# LOGOSOFT

telekomunikacijski sponsor

**HT ERONET**

oficijelni brend konferencije

**Lenovo**

gold sponzori

**Addiko Bank**

  
AUTHORITY PARTNERS

**bh**

 **COMTRADE**  
DISTRIBUTION

**EPSON**  
EXCEED YOUR VISION

**KimTec**

**LANACO**  
INFORMACIONE TEHNOLOGIJE

 **nsoft**

**PROINTER**  
IT SOLUTIONS AND SERVICES

  
**SEMOS**  
we can give you everything you need

 **sys company**

**teamwork**  
solution provider

**veeam**

silver sponzori

  
**Volkswagen**

**PORSCHE**  
SARAJEVO

  
**Audi**

 **APP IMPACT**  
impacting your business

**INFODOM**

  
**mistral**  
because it matters

**PHILIPS**  
Televizori

prijatelji konferencije

**communis**

 **FANFAN**

  
**GALAKTIKA**

**PROEVENT**

  
**SARAJEVO BUSINESS FORUM**

  
**UNIQA**

  
**WeAreDevelopers**

zvanično craft pivo

**BREW**

medijski sponzori

**akta**

 **ALJAZEERA**  
BALKANS

**20**  
stvbi.com

**Banke & Bizniš**

 **Banjaluka.com**  
—glavni banjalučki portal—

**BHRT**

 **bijesak info**  
by business people

**business**

**Dnevni list**

**FAKTOR**

**FBL**

**FENA** FEDERAL NEWS AGENCY

 **hayat.ba**

**HAYAT** | HD

**INFO**  
www.info.ba

 **Poduzetnik.ba**

**racunalo**  
www.racunalo.com

**REUNION**

**RSG**  
RADIO

**STUDENT**

**STUDOMAT**

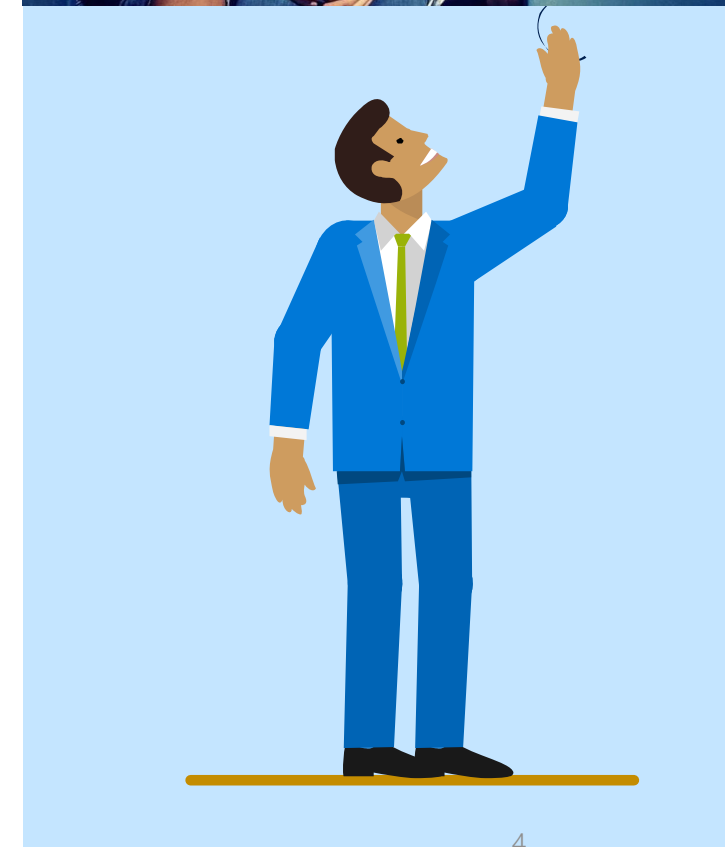
**TERMINAL**



# ... o predavaču



- ECS – Eurocomputer systems
  - Više od 20 godina u informatici
  - Logistika, metalurgija, prehrana, farmaceutika itd.
  - Cloud, privatni Cloud, On-Premise infrastruktura
  - Software Asset Management i upravljanje IT imovinom
  - MS Community u Hrvatskoj
  - Voditelj EDU ITPro i ITPro/NewOffice grupe
- 
- MVP – Office Servers and Services (Office 365)





# Agenda

- Malo o GDPR (General Data Protection Regulation)
  - Uredba o zaštiti podataka
- Microsoft i GDPR
  - Servisi unutar Office 365
- DEMO i više riječi o:
  - Compliance Manager
  - Demo DLP
  - Demo eDiscovery
  - Security Score
  - Office 365 Cloud Security



# GDPR – o čemu se tu radi?





# Tko bi trebao biti uključen u GDPR?

## Kratki upitnik

- |                      |                  |
|----------------------|------------------|
| • Legal department – | Pravna služba    |
| • Human Resources –  | Kadrovska služba |
| • IT department –    | IT služba/sektor |
| • Management –       | Uprava           |



# Tko bi trebao biti uključen u GDPR?

Kratki upitnik

- Legal department –
- Human Resources –
- Management –

Pravna služba

Kadrovska služba

Uprava

**Netko nedostaje!?**



# General Data Protection Regulation

## GDPR

- Novi evropski okvir za zaštitu osobnih podataka
- Značajne promjene u pravilima koja definiraju osobne podatke i kako se oni koriste
- Imenovanje (DPO – Data Protection Officer) koji će odgovarati izravno Upravi



# General Data Protection Regulation

... nastavak

## GDPR = General Data Protection Regulation

- Regulation (EU) 2016/679
- do 25. svibnja/maja 2018.

## Direktiva !!!

- Države članice moraju ju ugraditi u nacionalno zakonodavstvo



... ja sam van EU, mene se ne tiče?

- Ooo, da!!!

- Ako se obrađuju, zadržavaju ili spremaju osobni podaci bilo kojeg građanina EU...
  - Morate biti usklađeni sa GDPR-om
  - Bez obzira gdje ste!

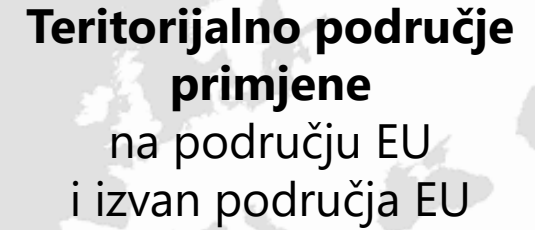


# Primjer privatnih podataka

- Osnovne identifikacijske informacije
  - kao ime, adresu i ID broj
- Web podaci
  - kao lokacija, IP adresa, cookie podaci i RFID tag
- Zdravstveni i genetički (genetski) podaci
  - Biometrijski podaci
- Rasa ili etnički podaci
- Politička mišljenja
- Seksualna orijentacija



# GDPR uloge



**Teritorijalno područje  
primjene**  
na području EU  
i izvan područja EU

- **Data kontrolor (Voditelj obrade)**

- Osoba ili agencija koja određuje svrhe i sredstva obrade osobnih podataka
  - Odlučuje kako će upravljati podacima (odlučuje o zaštiti podataka)

- **Data Procesor (Izvršitelj obrade)**

- Osoba ili agencija koja obrađuje osobne podatke u ime kontrolora

- **Data Protection Officer**

- daje smjernice za provedbu odgovarajućih mjera i brine o demonstraciji usklađenosti



# Zahtjev za pristup podacima

Uloga	Scenario
Građanin EU ili zaposlenik	Slanje zahtjeva za informaciju
Osoba zadužena za podatke (privatnost) – Privacy Officer	Otvaranje zahtjeva
Podrška zahtjevu (litigation)	Korištenje odgovarajućih alata za traženje podataka
Pravnik/odvjetnik ili služba za upravljanje	Analiziranje podataka
Privacy Officer	Šalje odgovor prema subjektu



# Gdje je tu Microsoft...

... i Office 365



# Gdje je tu Microsoft i Office 365

- Dana 15. februara 2017., Microsoft je objavio da će do 25. maja biti usklađen sa GDPR preporukama i regulativom
- <https://blogs.microsoft.com/on-the-issues/2017/02/15/get-gdpr-compliant-with-the-microsoft-cloud/>
- [Link](#)



# Podatkovna mjesta koja se mogu nadzirati

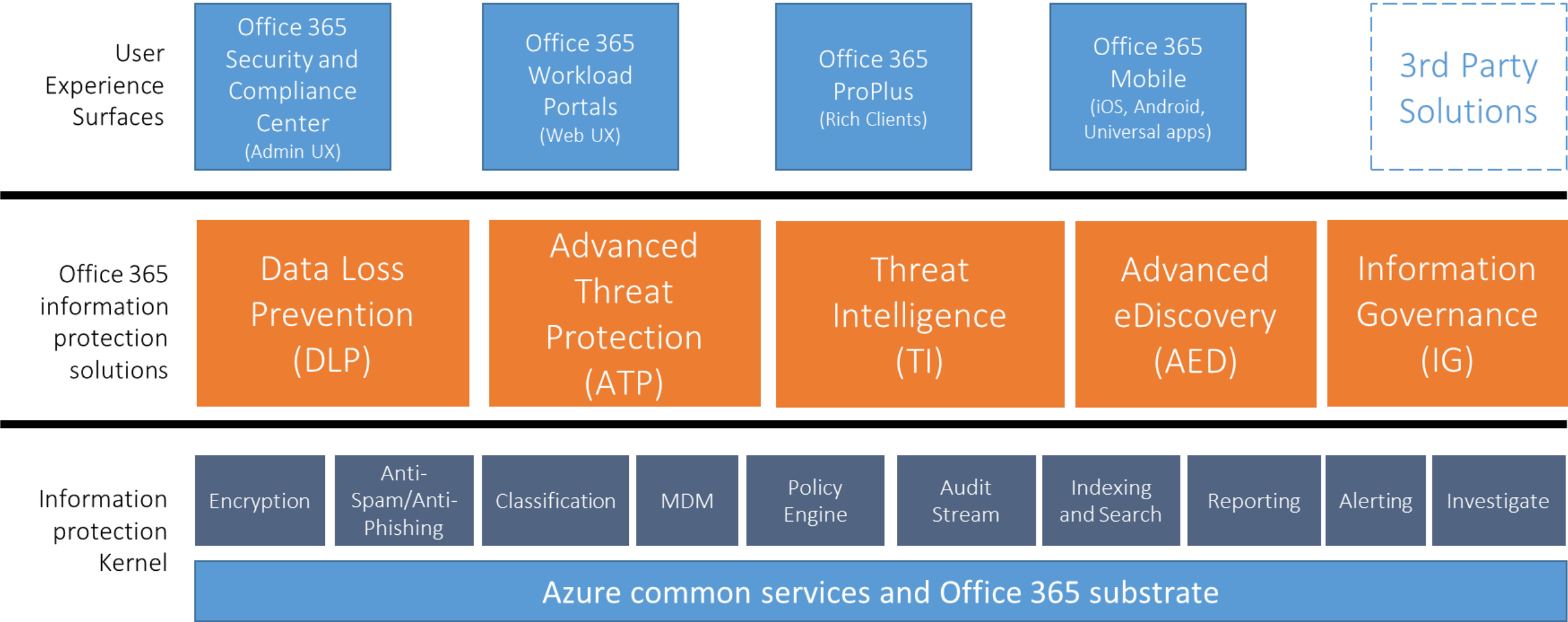
- Exchange – mail
- OneDrive for Business – dokumenti
- SharePoint Sites
- Skype for Business conversations
- Teams Data
- ... i ostalo



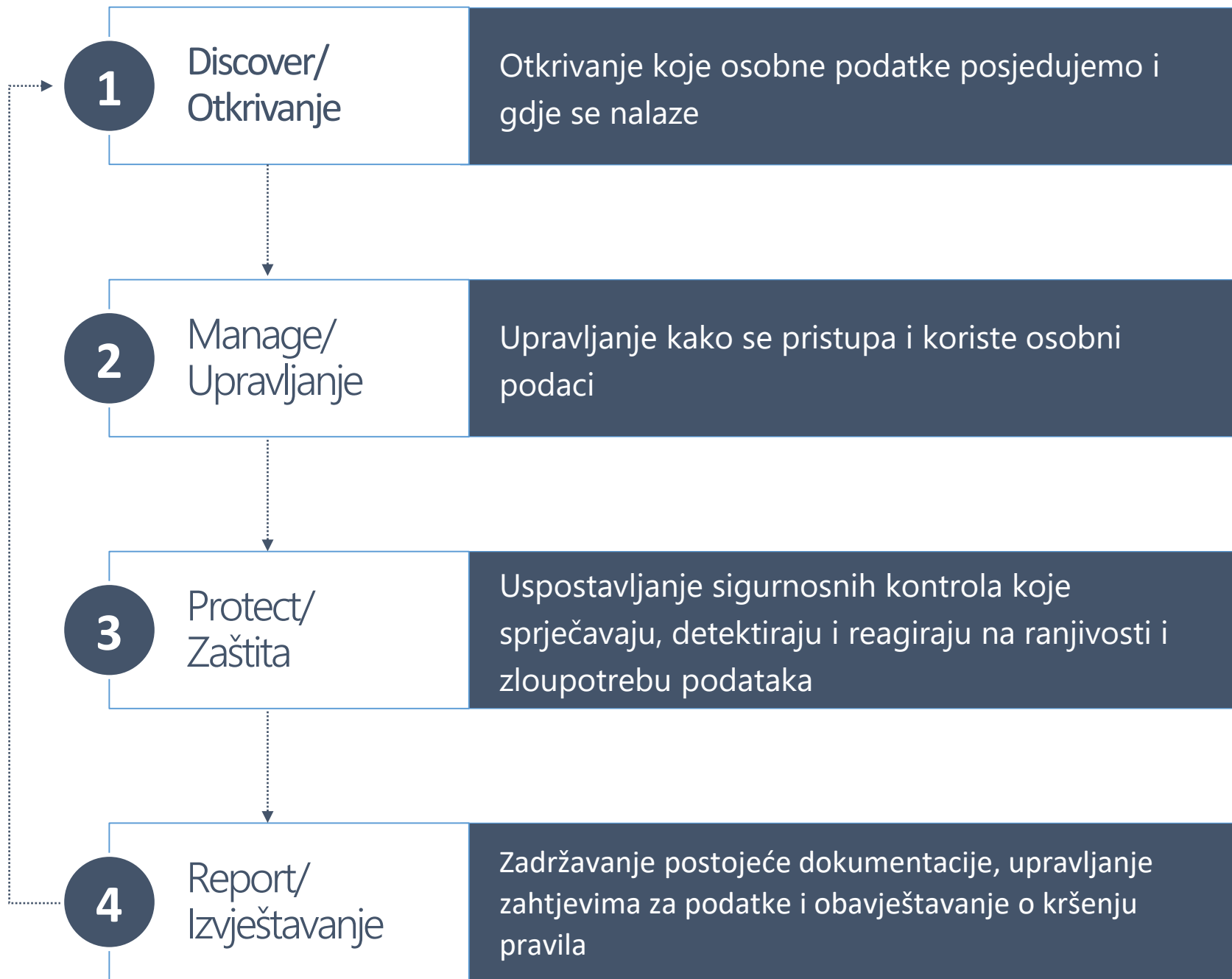
# Microsoft 365 i GDPR



# Office 365 - Security and Compliance Center









## ... podjela na faze

Discover /  
Otkrivanje

Manage /  
Upravljanje

Protect /  
Zaštita

Report /  
Izvještavanje

- Data Loss Prevention
- Advanced Data Governance
- Office 365 eDiscovery

- Advanced Data Governance
- Journaling (Exchange Online)

- Advanced Threat Protection
- Threat Intelligence

- Service Assurance
- Office 365 Audit Logs
- Customer Lockbox

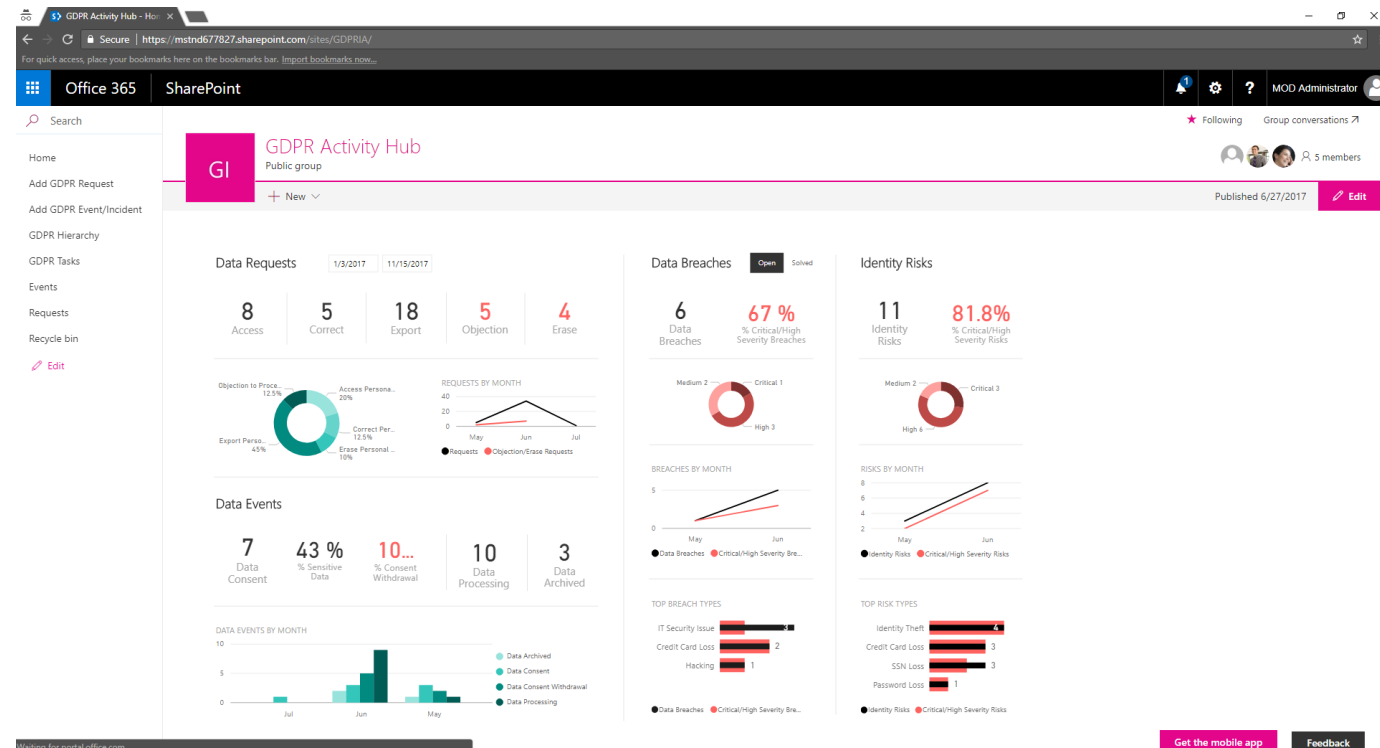


# Github – GDPR Activity Hub

- Open source projekt
- Starter kit za izgradnju upravljačkog centra

<https://github.com/SharePoint/sp-dev-gdpr-activity-hub>

- Pokazuje mogućnosti
  - SharePoint Framework
  - Office UI Fabric
  - Office 365 Developer Patterns





# 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?

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

↑ Import data

Bring data into Office 365 to safeguard it for GDPR.

🔍 Find personal data

Use content search to find and export personal data in your org.

⚙️ Govern

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

🏷️ Auto-apply labels

Automatically classify content containing personal data and make sure it's retained as needed.

🕒 Create a disposition label

Trigger disposition reviews so you can decide if personal data should be deleted when it reaches a certain age.

🛡️ Use Compliance Manager

Access your org's compliance posture for GDPR and get recommended actions for improvement.



# Demo...

... Compliance manager





Service Trust Portal

Guides ▾

Compliance Manager

meganb@william344.onmicrosoft.com ▾

# Compliance Manager

Compliance Reports

Trust Documents

Help ⓘ

Assessments

Action Items

Cloud

☐ Show Archived

+ Add Assessment

Filter Products ▾

Office 365  
GDPR

Actions ▾

Created 11/13/2017 Modified 11/13/2017

**Customer Controls** 0 of 48

**Microsoft Controls** 36 of 36

Office 365  
ISO 27001:2013

Actions ▾

Created 11/13/2017 Modified 11/13/2017

**Customer Controls** 0 of 71

**Microsoft Controls** 266 of 269

Office 365  
ISO 27018:2014

Actions ▾

Created 11/13/2017 Modified 11/13/2017

**Customer Controls** 0 of 23

**Microsoft Controls** 55 of 55

*Disclaimer: Compliance Manager is a dashboard that provides a summary of your data protection and compliance stature and recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate its effectiveness in your regulatory environment prior to implementation. Recommendations from Compliance Manager should not be interpreted as a guarantee of compliance.*



## Technical Support

Have a technical question on a Microsoft product or



## Frequently Asked Questions

Check the Microsoft Cloud Service Trust Portal FAQs



## Feedback

Service Trust Portal and Compliance

Feedback





Service Trust Portal

Guides

Compliance Manager

meganb@william344.onmicrosoft.com

< Back To Dashboard

EXPORT TO EXCEL

Office 365

GDPR

36/84



NotStarted

11/13/2017



Product

Framework

Compliant Controls

43% Assessed

Status

Last Modified

Assigned To

Office 365 in-Scope Cloud Services

Microsoft Managed Controls

Customer Managed Controls



## Technical Support

Have a technical question on a Microsoft product or service?



## Frequently Asked Questions

Check the Microsoft Cloud Service Trust Portal FAQs to see if your question has already been answered.



## Feedback

Service Trust Portal and Compliance Manager is currently in Preview and we need your feedback to make it as useful to you as possible.

Feedback sent





< Back To Dashboard

EXPORT TO EXCEL

Office 365

GDPR

36/84



NotStarted

11/13/2017



Product

Framework

Compliant Controls

43% Assessed

Status

Last Modified

Assigned To

### Office 365 in-Scope Cloud Services

The following services are included in this cloud service assessment.

- Sharepoint Online
- Exchange Online
- Microsoft Booking
- Microsoft Graph API
- Microsoft Analytics

- Microsoft Planner
- Microsoft Stream
- Office Delve
- Office 365 Groups
- Office 365 Video

- Sway
- Microsoft StaffHub
- Microsoft PowerApps
- Microsoft Teams
- Skype for Business

### Microsoft Managed Controls

### Customer Managed Controls



Feedback





< Back To Dashboard

EXPORT TO EXCEL

Office 365

GDPR

36/84



NotStarted

11/13/2017



Product

Framework

Compliant Controls

43% Assessed

Status

Last Modified

Assigned To

### Office 365 in-Scope Cloud Services

The following services are included in this cloud service assessment.

- Sharepoint Online
- Exchange Online
- Microsoft Booking
- Microsoft Graph API
- Microsoft Analytics
- Microsoft Planner
- Microsoft Stream
- Office Delve
- Office 365 Groups
- Office 365 Video
- Sway
- Microsoft StaffHub
- Microsoft PowerApps
- Microsoft Teams
- Skype for Business

### Microsoft Managed Controls

Access Control

1/1 Assessed

Authority and Purpose

1/1 Assessed

Accountability, Audit, and Risk

5/5 Assessed

Feedback



## Microsoft Managed Controls

Access Control



1/1 Assessed

Authority and Purpose

1/1 Assessed

Accountability, Audit, and Risk

5/5 Assessed

MS Control	Certification Control(s)	Description	Status	Test Date	Test Result
AR-0104	GDPR: Article 24(1)	<p>GDPR</p> <ul style="list-style-type: none"><li>Article 24(1): Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.</li></ul>	Implemented	10/19/2016  Tested By Third Party Independent Auditor	 Passed
AR-0110	GDPR: Article 28(3)(g), Article 28(3)(a), Article 28(3)(e), Article 47(2)(g)	<p>GDPR</p> <p>Article 28(3)(g): Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;</p> <p>Article 28(3)(a): Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;</p>	Implemented	10/19/2016  Tested By Third Party Independent Auditor	 Passed

Feedback



Authority and Purpose

1/1 Assessed

Accountability, Audit, and Risk

5/5 Assessed

MS Control	Certification Control(s)	Description	Status	Test Date	Test Result
AR-0104	GDPR: Article 24(1)	GDPR <ul style="list-style-type: none"> <li>Article 24(1): Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.</li> </ul>	Implemented	10/19/2016  Tested By Third Party Independant Auditor	<div> </div> Passed

Less

Microsoft Implementation Details		Test Plan Details	Management Response	
<p>Microsoft management demonstrates leadership and commitment with respect to the Office 365 Information Security Management System (ISMS) by ensuring that information security policies and objectives are established and are compatible with the strategic direction of Microsoft. Microsoft establishes, implements, maintains, and continually improves its ISMS, in accordance with the requirements of international standards. Microsoft develops, documents, and disseminates a security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Microsoft and Office 365 security policies exist in order to provide Office 365 staff and contractor staff with a current set of clear and concise information security policies. These policies provide direction for the appropriate protection of Office 365. Further an Office 365 Information Security Policy has been created as a component of an overall ISMS for Office 365. The Office 365 Information Security Policy has been reviewed, approved, and</p> <p>Read More</p>		<p>Reviewed and validated that the following policies exist and confirmed that the documents demonstrate leadership and commitment with respect to the Office 365 ISMS by ensuring that the information security policy and the information security objectives are established and are compatible with the strategic direction of Microsoft. Examined Office 365 information security policies and standard operating procedures (SOPs), and determined that Microsoft's information security program is built around the purpose of protecting the confidentiality, integrity, availability, and reliability of Office 365 information systems and data.</p> <p>Interviewed Office 365 Security and Trust team leads, and determined that Office 365 has developed a control framework to achieve intended outcome of its ISMS.</p> <p>In addition, reviewed samples of the associated policies and confirmed that these documents provide additional granularity and policy clarification (engineering guidance) and</p> <p>Read More</p>	N/A	
AR-0110	GDPR: Article 28(3)(g), Article 28(3)(a), Article 28(3)(e), Article 47(2)(g)	GDPR Article 28(3)(g): Processing by a processor shall be governed by a	Implemented	10/19/2016  Tested By:

Feedback





[◀ Back To Dashboard](#)

EXPORT TO EXCEL

Office 365

GDPR

36/84



NotStarted

11/13/2017



Product

Framework

Compliant Controls

43% Assessed

Status

Last Modified

Assigned To

### Office 365 in-Scope Cloud Services

The following services are included in this cloud service assessment.

- Sharepoint Online
- Exchange Online
- Microsoft Booking
- Microsoft Graph API
- Microsoft Analytics
- Microsoft Planner
- Microsoft Stream
- Office Delve
- Office 365 Groups
- Office 365 Video
- Sway
- Microsoft StaffHub
- Microsoft PowerApps
- Microsoft Teams
- Skype for Business

### Microsoft Managed Controls

### Customer Managed Controls



Feedback



## Customer Managed Controls ^

Access Control	0/1 Assessed <span>∨</span>
Authority and Purpose	0/2 Assessed <span>∨</span>
Accountability, Audit, and Risk	0/13 Assessed <span>∨</span>
Audit and Accountability	0/1 Assessed <span>∨</span>
Data Minimization and Retention	0/4 Assessed <span>∨</span>
Incident Response	0/4 Assessed <span>∨</span>
Individual Participation and Redress	0/10 Assessed <span>∨</span>
Personnel Security	0/1 Assessed <span>∨</span>
Program Management	0/1 Assessed <span>∨</span>
Risk Assessment	0/2 Assessed <span>∨</span>
Security Assessment	0/1 Assessed <span>∨</span>
System and Communication Security	0/2 Assessed <span>∨</span>
System and Services Acquisition	0/1 Assessed <span>∨</span>

Feedback



## Incident Response

0/4 Assessed

## Individual Participation and Redress

0/10 Assessed

MS Control	Certification Control(s)	Description	Assigned To	Status	Test Date	Test Result
IP-0100	... GDPR: Article 6(1)(a), Article 7(1)	<p>GDPR</p> <ul style="list-style-type: none"><li>Article 6(1)(a): Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;</li><li>Article 7(1): Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.</li></ul>	<a href="#">Assign</a> Manage Documents	Select ▾	<input type="text"/>	Select ▾
More ▾						
IP-0102	... GDPR: Article 15(3)	<p>GDPR</p> <ul style="list-style-type: none"><li>Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.</li></ul>	<a href="#">Assign</a> Manage Documents	Select ▾	<input type="text"/>	Select ▾
More ▾						
IP-0103	... GDPR: Article 15(3)	<p>GDPR</p> <ul style="list-style-type: none"><li>Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.</li></ul>	<a href="#">Assign</a> Manage Documents	Select ▾	<input type="text"/>	Select ▾
More ▾						
IP-0105	... GDPR: Article 12(5)	<p>GDPR</p> <p>Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller</p>	<a href="#">Assign</a> Manage Documents	Select ▾	<input type="text"/>	Select ▾

Feedback



shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

More 

IP-0102 ... [GDPR: Article 15\(3\)](#)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

Assign

Select 

Manage Documents

Select Less 

### Customer Actions

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you to classify data across your organization for governance, and to enforce retention rules based on that classification.

Once Labels have been assigned to content, either by users or auto-applied, you can use Content Search in the Security & Compliance Center to find all content that's classified with a specific label.

Content Search can also be used to provide a copy of a user's personal data in response to a request from a data subject. Content Search can be used to locate items such as email, documents, and instant messaging conversations in Exchange.

[Read More](#)

## Implementation Details

You can enter implementation details and related notes in this field as you implement this control. Along with Microsoft provided customer actions, details entered by you help team members in your organization as well as auditors / regulators to understand how you implemented this control and how they can test this control.

## Test Plan & Management Response


You can enter test plan here to track how you plan to test this controls and track your test results details along with management response and risk assessment for the control where you had any findings.

IP-0103 ... GDPR: Article 15(3)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a

## Assign

Select 

Manage Documents

Select 

## Feedback



Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using [Labels](#) in Office 365. Labels enable you to classify data across your organization for governance, and to enforce retention rules based on that classification.

Once Labels have been assigned to content, either by users or auto-applied, you can use [Content Search](#) in the Security & Compliance Center to find all content that's classified with a specific label.

Content Search can also be used to provide a copy of a user's personal data in response to a request from a data subject. Content Search can be used to locate items such as email, documents, and instant messaging conversations in Exchange Online mailboxes and public folders, SharePoint Online, OneDrive for Business, Skype for Business, Teams, and Groups. The first step is to starting using the Content Search tool to choose content locations to search and configure a keyword query to search for specific items. Or, you can just leave the query blank and return all items in the target locations.

In addition to performing data classification and to search for content in Office 365, there are some general process/workflow-related steps you can also perform to satisfy the requirements for this article. This includes submitting and tracking the status of the data request(s) and handling feedback from the data subject, which can be done using feature found in Exchange Online, SharePoint Online, Office Online, and other cloud services, as well as optionally charging a fee to the Data Subject for processing additional requests.

Office 365 includes several features that can be used to facilitate compliance of the requirements of this article, including [Advanced Data Governance](#), which allows you to retain important information and delete unimportant information by classifying information based on a retention or deletion policy or both. It includes intelligent/automated actions such as recommending policies; automatically applying labels to data; applying labels based on sensitive data types or queries; and use of smart import filters. It also includes the Supervision feature for reviewing employee communications for security and compliance purposes. implementing data classification for content in your organization, and executing content searches.

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the

Select 

Manage Documents

Select 

Customers are not  
their users, custo  
copies of person

To facilitate more effective data management, Microsoft recommends using the new classification system to classify data across the organization and enforce retention policies.

Once Labels have auto-applied, you can add a Compliance Certificate specific label.

Content Search  
personal data in  
Content Search  
documents, and

[Read More](#)

IP-0103 ... GDPR: Article 15(3)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a

Select 

Manage Documents

Select 



shall be able to demonstrate that the data subject has consented to processing of his or her personal data.


More 


IP-0102 ... GDPR: Article 15(3)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

Assign  
Manage Documents

Select 

Select 

Less 

#### Customer Actions

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you to classify data across your organization for governance, and to enforce retention rules based on that classification.

Once Labels have been assigned to content, either by users or auto-applied, you can use Content Search in the Security & Compliance Center to find all content that's classified with a specific label.

Content Search can also be used to provide a copy of a user's personal data in response to a request from a data subject. Content Search can be used to locate items such as email, documents, and instant messaging conversations in Exchange

[Read More](#)

#### Implementation Details

You can enter implementation details and related notes in this field as you implement this control. Along with Microsoft provided customer actions, details entered by you help team members in your organization as well as auditors / regulators to understand how you implemented this control and how they can test this control.

#### Test Plan & Management Response


You can enter test plan here to track how you plan to test this controls and track your test results details along with management response and risk assessment for the control where you had any findings.

IP-0103 ... GDPR: Article 15(3)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a

Assign  
Manage Documents

Select 

Select 

Feedback



- Article 7(1): Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

More

IP-0102 ... GDPR: Article 15(3)

GDPR

Assign

Select

Select

### Assign Task

Assign To

MS Control:

IP-0102

Customer Actions:

Select Priority

Select an Option

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you to track how you plan to test this and results details along with risk assessment for the control.

Read More

☒ Send email notification

Assign Task Notes:

Add notes here...

Cancel

Assign

#### Customer Actions

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you to track how you plan to test this and results details along with risk assessment for the control.

Once Labels have been assigned to content, they are auto-applied, you can use Content Search in the Compliance Center to find all content with a specific label.

Content Search can also be used to provide a response to a request for personal data in response to a request. Content Search can be used to locate information in documents, and instant messaging conversations.

Read More

IP-0103 ... GDPR: Article 15(3)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the

Assign

Select

Select

Manage Documents

Feedback



- Article 7(1): Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

More

IP-0102 ... GDPR: Article 15(3)

GDPR

Assign

Select

Select

## Assign Task

Assign To

allan

AD Allan Deyong

Select an Option

MS Control:

IP-0102

Customer Actions:

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you to track how you plan to test this and results details along with risk assessment for the control.

[Read More](#)

☒ Send email notification

Assign Task Notes:

Add notes here...

Cancel

Assign

IP-0103 ... GDPR: Article 15(3)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the

Assign

Select

Select

Manage Documents

Feedback



- Article 7(1): Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

More

IP-0102 ... GDPR: Article 15(3)

GDPR

Assign

Select

Select

## Assign Task

Assign To

AD Allan Deyoung

MS Control:

IP-0102

Customer Actions:

Select Priority

Select an Option

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you to track how you plan to test this and results details along with risk assessment for the control.

Read More

☒ Send email notification

Assign Task Notes:

Add notes here...

Cancel

Assign

### Customer Actions

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you to track how you plan to test this and results details along with risk assessment for the control.

Once Labels have been assigned to content, you can use Content Search to find all content that is associated with a specific label.

Content Search can also be used to locate and delete personal data in response to a request. Content Search can be used to locate and delete documents, and instant messaging conversations.

Read More

IP-0103 ... GDPR: Article 15(3)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the

Assign

Select

Select

Manage Documents

Feedback



- Article 7(1): Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

More

IP-0102 ... GDPR: Article 15(3)

GDPR

Assign

Select

Select

### Assign Task

Assign To

AD Allan Deyoung

MS Control:

IP-0102

Customer Actions:

Select Priority

Select an Option

Low

Medium

High

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you

[Read More](#)

☒ Send email notification

Assign Task Notes:

Add notes here...

Cancel

Assign

#### Customer Actions

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you to enforce retention rules based on that classification.

Once Labels have been assigned to content, they are auto-applied, you can use Content Search in the Compliance Center to find all content with a specific label.

Content Search can also be used to provide a list of personal data in response to a request. Content Search can be used to locate information in documents, and instant messaging conversations.

[Read More](#)

#### Response

Use this section to track how you plan to test this control. It results details along with the control risk assessment for the control.

IP-0103 ... GDPR: Article 15(3)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the

Assign

Select

Select

Manage Documents

Feedback



- Article 7(1): Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

More

IP-0102 ... GDPR: Article 15(3)

GDPR

Assign

Select

Select

### Assign Task

Assign To

AD Allan Deyoung

MS Control:

IP-0102

Customer Actions:

Select Priority

High

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you to track how you plan to test this and results details along with risk assessment for the control.

☒ Send email notification

Assign Task Notes:

Please follow the recommended actions to design a business process for data subject requests and provide evidence.

Cancel

Assign

#### Customer Actions

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you to track how you plan to test this and results details along with risk assessment for the control.

Once Labels have been assigned to content, they are auto-applied, you can use Content Search in the Compliance Center to find all content associated with a specific label.

Content Search can also be used to provide a response to a request for personal data in response to a request. Content Search can be used to locate content in documents, and instant messaging conversations.

Read More

IP-0103 ... GDPR: Article 15(3)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the

Assign

Select

Select

Manage Documents

Feedback



- Article 7(1): Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

More ▾

IP-0102 ... GDPR: Article 15(3)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.



Manage Documents

Select ▾



Select ▾

Less ▲

### Customer Actions

Customers are responsible for responding to requests from their users, customers, and other individuals (data subjects) for copies of personal data undergoing processing.

To facilitate monitoring of compliance for this article, Microsoft recommends that your organization implement data classification using Labels in Office 365. Labels enable you to classify data across your organization for governance, and to enforce retention rules based on that classification.

Once Labels have been assigned to content, either by users or auto-applied, you can use Content Search in the Security & Compliance Center to find all content that's classified with a specific label.

Content Search can also be used to provide a copy of a user's personal data in response to a request from a data subject. Content Search can be used to locate items such as email, documents, and instant messaging conversations in Exchange

[Read More](#)

### Implementation Details

You can enter implementation details and related notes in this field as you implement this control. Along with Microsoft provided customer actions, details entered by you help team members in your organization as well as auditors / regulators to understand how you implemented this control and how they can test this control.

### Test Plan & Management Response

You can enter test plan here to track how you plan to test this controls and track your test results details along with management response and risk assessment for the control where you had any findings.

IP-0103 ... GDPR: Article 15(3)

GDPR

- Article 15(3): The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the

Assign

Select ▾



Select ▾

Manage Documents

Feedback



# Data Loss Prevention - DLP



# Data Loss Prevention - DLP

- Zaštita informacija
- Usmjeravanje korisnika na važnost podataka
- Većina informacija slučajno „iscuri”
- Nevidljivi servis koji odraduje svoj posao prema zahtjevima poslovanja



# DLP mehanizam

## Ugrađeni servis u Office 365 (Exchange i SP u prošlosti)

- Izrada pravila
- Predefinirana pravila
- Vlastita pravila

## Definiranje ponašanja kada se dogodi detekcija

- Obavijest
- Akcija
- Izvještavanje



# Secure Score

Servis koji nadgleda vaš Office 365 Tenant

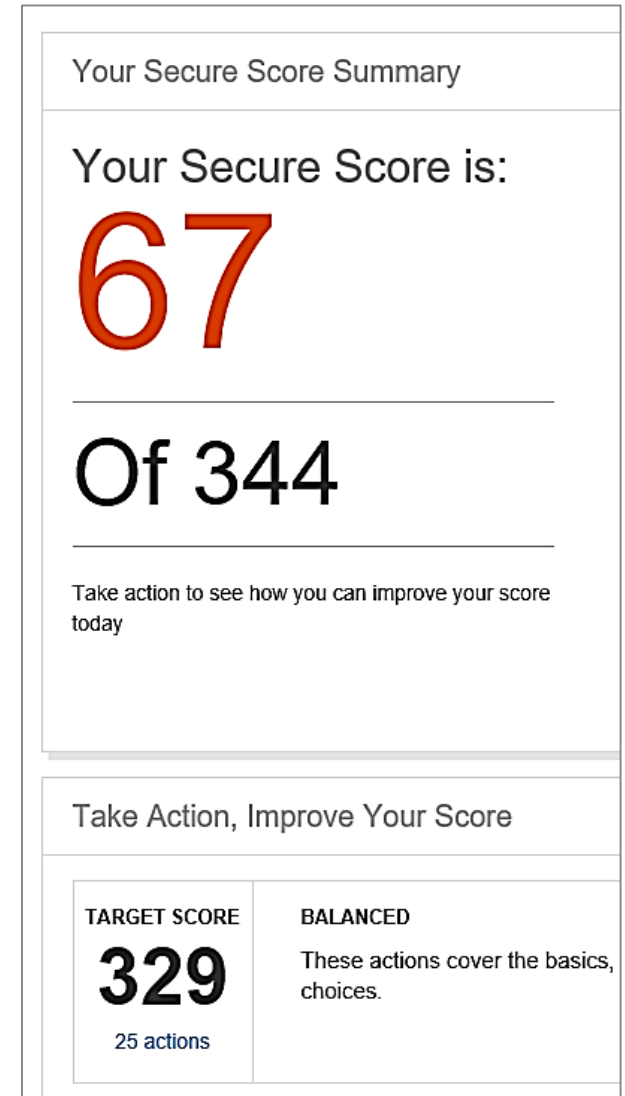
- <https://securescore.office.com>

Kako radi:

- Logiranje s administratorskim računom
- Global Administrator ili Custom Administrator role

Podržani Office 365 paketi:

- Business Premium
- Enterprise



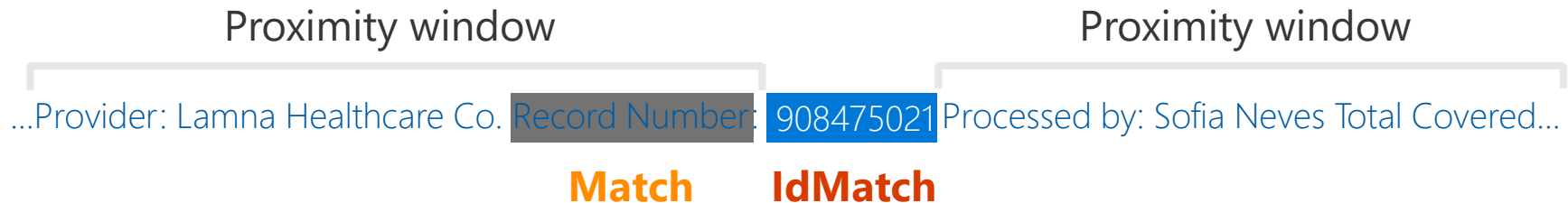


# Način detekcije - validacija

Uobičajene metode - Matrica/Pattern  
Karakteristi, podešavanje, checksum

Dodatno dokazivanje - provjera

Približno prepoznavanje – heuristika, validacija (Proximity)  
Ključne riječi, datumi, ostale matrice i ostalo





# DLP – primjer matrice

Croatia Identity Card Number	
<b>Format</b>	Nine digits
<b>Pattern</b>	Nine consecutive digits
<b>Checksum</b>	No
<b>Definition</b>	<p>A DLP policy is 75% confident that it's detected this type of sensitive information if, within a proximity of 300 characters:</p> <ul style="list-style-type: none"><li>▪ The function <code>Func_croatia_id_card</code> finds content that matches the pattern.</li><li>▪ A keyword from <code>Keyword_croatia_id_card</code> is found.</li></ul> <pre>&lt;!--Croatia Identity Card Number--&gt; &lt;Entity id="ff12f884-c20a-4189-b185-34c8e7258d47" recommendedConfidence="75" patternsProximity="300"&gt;   &lt;Pattern confidenceLevel="75"&gt;     &lt;IdMatch idRef="Func_croatia_id_card"/&gt;     &lt;Match idRef="Keyword_croatia_id_card"/&gt;   &lt;/Pattern&gt; &lt;/Entity&gt;</pre>
<b>Keywords</b>	<div>Keyword_croatia_id_card</div> <div>Croatian identity card</div> <div>Osobna iskaznica</div>

Croatia Personal Identification (OIB) Number	
<b>Format</b>	10 digits
<b>Pattern</b>	<p>10 digits:</p> <ul style="list-style-type: none"><li>▪ Six digits in the form DDMMYY which are the date of birth</li><li>▪ Four digits where the final digit is a check digit</li></ul>
<b>Checksum</b>	Yes
<b>Definition</b>	<p>A DLP policy is 85% confident that it's detected this type of sensitive information if, within a proximity of 300 characters:</p> <ul style="list-style-type: none"><li>▪ The function <code>Func_croatia_oib_number</code> finds content that matches the pattern.</li><li>▪ A keyword from <code>Keyword_croatia_oib_number</code> is found.</li><li>▪ The checksum passes.</li></ul> <p>A DLP policy is 75% confident that it's detected this type of sensitive information if, within a proximity of 300 characters:</p> <ul style="list-style-type: none"><li>▪ The function <code>Func_croatia_oib_number</code> finds content that matches the pattern.</li><li>▪ The checksum passes.</li></ul> <pre>&lt;!-- Croatia Personal Identification (OIB) Number --&gt; &lt;Entity id="31983b6d-db95-4eb2-a630-b44bd091968d" recommendedConfidence="85" patternsProximity="300"&gt;   &lt;Pattern confidenceLevel="85"&gt;     &lt;IdMatch idRef="Func_croatia_oib_number"/&gt;     &lt;Match idRef="Keyword_croatia_oib_number"/&gt;   &lt;/Pattern&gt;   &lt;Pattern confidenceLevel="75"&gt;     &lt;IdMatch idRef="Func_croatia_oib_number"/&gt;   &lt;/Pattern&gt; &lt;/Entity&gt;</pre>
<b>Keywords</b>	<div>Keyword_croatia_oib_number</div> <div>Personal Identification Number</div>

- [https://technet.microsoft.com/en-us/library/jj150541\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/jj150541(v=exchg.160).aspx)



# DLP pravila

The image shows a screenshot of the Microsoft DLP (Data Loss Prevention) policy configuration interface. The interface is divided into several sections:

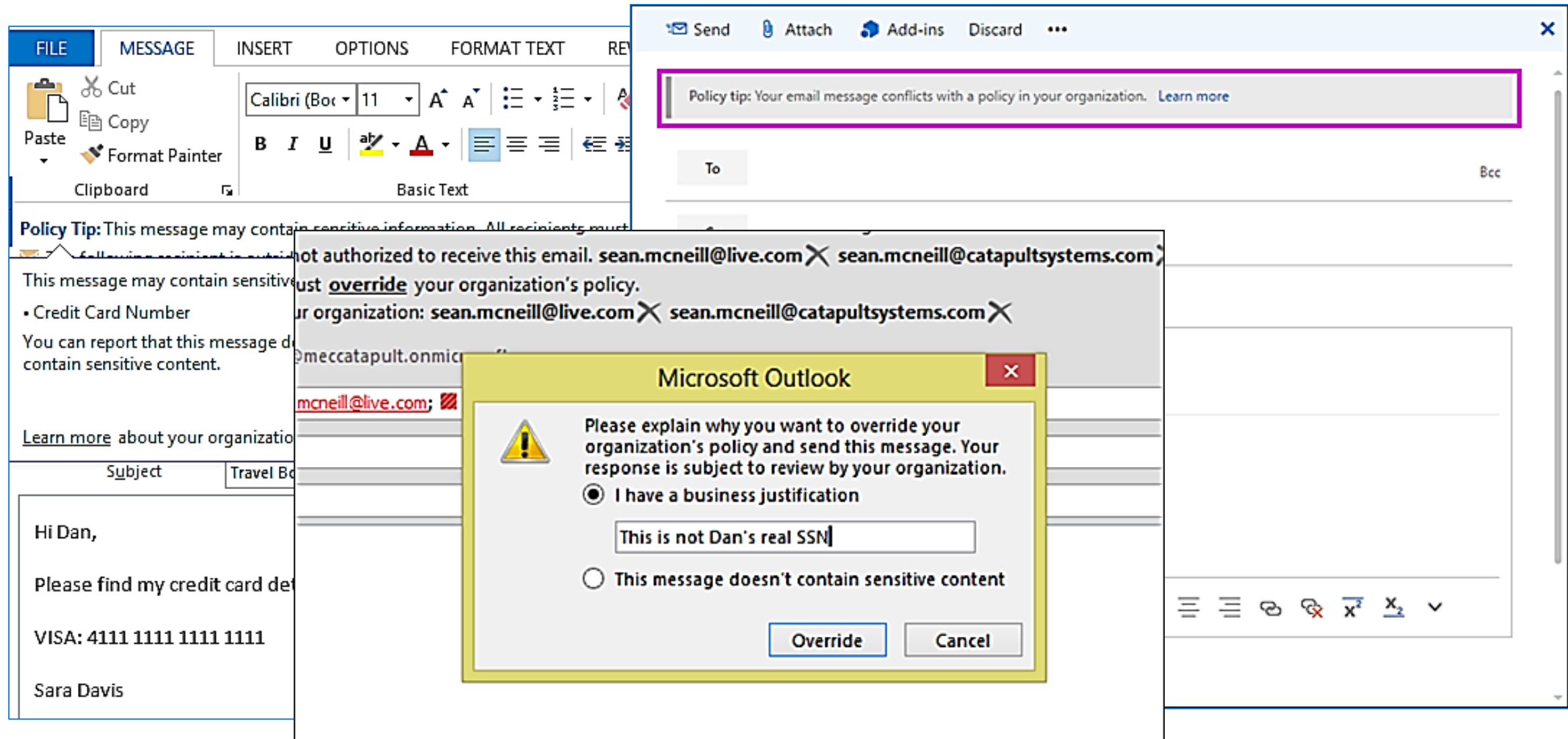
- Conditions:** This section allows users to define what kind of content triggers a policy. It includes a dropdown menu for "Conditions" and a button labeled "Add or change types". A tooltip indicates "When content contains sensitive information".
- Actions:** This section allows users to define what happens when a policy match occurs. It includes a dropdown menu for "Actions" and a button labeled "Add a condition". A tooltip indicates "Content is shared".
- Incident reports:** This section allows users to configure how incident reports are generated and sent. It includes a dropdown menu for "Incident reports" and a button labeled "Add or remove people".

Key configuration options visible include:

- Severity level:** A dropdown menu set to "Low".
- Email incident reports:** A toggle switch turned on, with a tooltip "Toggle this to turn on incident reports."
- Send notifications to these people:** A list of email addresses, currently showing "admin@alpinehouse.onmicrosoft.com".
- User notifications:** A section with a toggle switch turned on, a radio button for "Notify the user who sent, shared, or received the content", and checkboxes for "Customize the email text" and "Customize the policy tip text".
- User overrides:** A section with a toggle switch turned on, a checkbox for "Require a business justification to override the policy", and a checkbox for "Override the rule automatically if the policy is violated".



# DLP – policy tips





# eDiscovery - eOtkrivanje



# eDiscovery - eOtkrivanje

Content search > Search : Dalekovod

Search Export

Back to saved searches

+ New search

Search query

Keywords

Dalekovod

Show keyword list

Sender

Contains any of

dalekovod

Locations: selected

All locations

Specific locations

Status: completed

Save & run

Notice something different? Our eDiscovery experience is new and improved. [Learn more about it.](#)

Refresh Search

Name	Last export start time	Exported by	Searches
Dalekovod_Export	2017-12-07 11:02:30	Tomislav Lulić	Dalekovod
Dalekovod_ReportsOnly	2017-12-07 11:01:34	Tomislav Lulić	Dalekovod
DLP search_Export	2017-12-03 21:47:07	Tomislav Lulić	DLP search
FAG_Export	2017-12-03 21:41:44	Tomislav Lulić	FAG
FAG_ReportsOnly	2017-10-23 06:41:04	Tomislav Lulić	FAG
DLP search_ReportsOnly	2017-04-25 23:46:36	Tomislav Lulić	DLP search



# Security score i dokumentacija



# Service Assurance – skup dokumenata

Home > Dashboard

**Service assurance**

Service Assurance provides information about the controls and how they are implemented in Office 365, and Dynamics 365, and gain confidence in the security of your data and gain confidence in compliance, audit, and availability to them.

**What's new**

**Audited Controls**  
This feature is designed to help you understand the controls and how they are implemented in Office 365, and Dynamics 365, and gain confidence in the security of your data and gain confidence in compliance, audit, and availability to them.

**SOC and ISO audit reports**  
We now have SOC and ISO audit reports for Office 365, and Dynamics 365, and Yammer, and testing for Data Transfer and Replication & Data Transfer.

**Customer Security Checklist**  
This workbook is designed to help you consider the features to consider for your organization.

Home > Audited controls

**Status of audited controls**

Use this page to understand the controls and how they are implemented in Office 365, and Dynamics 365, and gain confidence in the security of your data and gain confidence in compliance, audit, and availability to them.

[Download](#)

☐ **Standard/Regulation**

☐ **ISO 27001-2013**  
Office 365 has been audited under this standard. Information Security Management System (ISMS) implementation and availability of your data.

☐ **ISO 27018-2014**  
In line with Office 365 has been audited under this standard. Information Security Management System (ISMS) implementation and availability of your data.

☐ **NIST 800-53A (Rev. 4)**  
Office 365 has been audited under this standard. Information Security Management System (ISMS) implementation and availability of your data.

Home > Trust documents

**Trust documents provided by Microsoft**

Understand how Microsoft cloud services protect your data and your organization's information.

**FAQ and White Papers**

View answers to frequently asked questions and white papers.

About Microsoft Cloud Security  
Assessing Risk in the Microsoft Cloud and Getting Answers to  
Auditing and Reporting in Office 365  
Azure - Cloud Security Diagnostic Tool 2016  
Azure - NIST CSF Enablement\_Detect Function  
Azure - NIST CSF Enablement\_Protect Function  
Azure - NIST CSF Risk Assessment Checklist  
Azure 13 Effective Security Controls for ISO 27001 Compliance  
Azure A Practical Guide to Designing Secure Health Solutions  
Azure Advanced Threat Detection  
Azure Blueprint DFARS Customer Responsibilities Matrix  
Azure Blueprint DoD L4 Customer Responsibilities Matrix  
Azure Blueprint DoD L4 SSP  
Azure Blueprint DoD L5 Customer Responsibilities Matrix  
Azure Blueprint DoD L5 SSP  
Azure Blueprint FedRAMP High Customer Responsibilities Matrix  
Azure Blueprint FedRAMP High SSP  
Azure Blueprint FedRAMP Moderate Customer Responsibilities Matrix  
Azure Blueprint FedRAMP Moderate SSP  
Azure Blueprint HITRUST Customer Responsibilities Matrix  
Azure Blueprint NIST CSF Customer Responsibilities Matrix  
Azure Blueprint NIST SP 800-171 Customer Responsibilities Matrix  
Azure Blueprint NIST SP 800-53 Implementation Guide  
Azure Blueprint NIST SP 800-66 HIPAA Customer Responsibilities Matrix  
Azure Blueprint UK G-Cloud Customer Responsibilities Matrix  
Azure Blueprint UK G-Cloud SSP  
Azure Cloud Platform Hardening Guide  
Azure Data Classification for Cloud Readiness

Home > Compliance reports

**Service compliance reports**

Third party independent audit and GRC assessment reports for Microsoft cloud services. Stay up to date on how Microsoft cloud services comply with global standards that matter to your organization.

**FedRAMP Reports**

**GRC Assessment Reports**

**ISO Reports**

ISO information security management related reports for Microsoft Cloud Services.

Azure - ISO 22301 Audit Assessment Report  
Azure - ISO 27001 and ISO 27018 Audit Assessment Report 2017  
Azure - ISO 27001 and ISO 27018 Audit Statement of Applicability (SOA) 2017  
Azure - ISO 27017 - Code of practice for information security controls - Certificate  
Azure - Microsoft Cloud Infrastructure Operations ISO 22301 - Business Continuity Management Standard - Certificate  
Azure - Microsoft ISO 9001 Assessment Report 2017  
Azure - Microsoft ISO 9001 Certificate 2017  
Azure and Power BI ISO 27001 Audit Assessment Certificate  
Azure and Power BI ISO 27018 Audit Assessment Certificate  
Azure CY17 ISO 27001 Certificate - IS 577753  
Azure FY17 - ISO 20000-1 Certificate  
Azure FY17 ISO 20000-1 Statement of Applicability  
Azure FY17 ISO 27017 Assessment Report  
Azure FY17 ISO 27017 Certificate  
Azure FY17 ISO 27017 Statement of Applicability  
Azure Germany ISO 27001 Certificate 44121161106 Year 2017  
Azure Germany ISO 27018 Certificate 44999161106 Year 2017  
Azure ISO 27001 Certificate IS 577753 Year 2016  
Azure ISO 27001\_27018 Assessment Report Year 2016



# Office 365 Cloud App Security



# Office 365 Cloud App Security

- Office 365 E5

Što donosi:

- Obavijesti – kreiranje obavijesti i pretraga anomalija i poremećaja u funkcioniranju
- Otkrivanje produktivnosti aplikacija – pregled korištenja i načina korištenja servisa i aplikacija
- Prava aplikacija – pregled i kontrola aplikacija koje imaju pristup O365 okruženju
- EU data centar



# Danas smo pričali o...

Malo o GDPR-u (General Data Protection Regulation)

Demo

- Demo DLP
- Demo eDiscovery

Compliance Manager

Prikaz Security Score ...



# Slijedeći koraci...



Započnite GDPR procjenom:  
<http://aka.ms/gdprassessment>



Procjenite vaš rizik sa Compliance Manager  
<https://aka.ms/compliancemanager>



Klasificirajte svoje podatke s Azure AIP  
i uvedite Office 365 ATP





# HVALA!



@tlulic



<https://tlulic.wordpress.com>



[tomislav@tlulic.com](mailto:tomislav@tlulic.com)



<https://hr.linkedin.com/in/tomislavlulic>



# GDPR linkovi

What GDPR means to Office 365

- <https://www.petri.com/gdpr-office-365>

EU GDPR

- <http://www.eugdpr.org/>

MS compliance

- <https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Manage-Your-Compliance-from-One-Place-Announcing-Compliance/ba-p/106493>

GDPR

- <https://www.petri.com/gdpr-office-365>
- <https://britishlegalitforum.com/news/general-data-protection-regulation-gdpr-compliance-magic-bullet/>
- <https://www.analyticsinhr.com/blog/general-data-protection-regulation-gdpr-impact-hr-analytics/>
- <https://www.csoononline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html>



