



Microsoft Teams and GDPR

Advice and Compliance
(today live from Dresden)

Thomas Poett
Office Server and Services MVP



Agenda GDPR with MS Teams



- GDPR Generic Overview
- Threads in MS Teams
- Compliance Control in Office 365
- Applying in MS Teams



GDPR Generic Overview



GDPR

General Data Protection
Regulation

DSVGO

DatenSchutz
GrundVerOrdnung

The GDPR aims primarily to **give control back to citizens and residents over their personal data** and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect, it will replace the data protection directive (officially Directive 95/46/EC) of 1995.

The regulation was adopted on 27 April 2016. It becomes enforceable from 25 May 2018 after a two-year transition period and, unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable

Where does GDPR apply



GDPR is a regulation that requires businesses to protect the **personal data and privacy of EU citizens** for transactions that occur within EU member states.

<https://www.eugdpr.org/>

Data breaches which may pose a risk to individuals must be notified to the **DPA within 72 hours** and **to affected individuals without undue delay**.

GDPR Compliance Support with Microsoft



Updates in Microsoft 365—help protect sensitive data and include:

- **Compliance Manager** general availability for Azure, Dynamics 365, and Office 365 Business and Enterprise customers in public clouds.
- **Compliance Score** availability for Office 365.
- **Azure Information Protection** scanner general availability.

In addition, capabilities in Microsoft 365 help to:

- Protect sensitive data in apps and across cloud services.
- Support data protection across platforms.
- Provide a consistent labeling schema experience.

Talking about Protect (with MS Teams)



4 STEP's in GDPR compliance



Discover

Identify which personal data you have and where it resides >



Manage

Govern how personal data is used and accessed >



Protect

Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches >



Report

Keep required documentation and manage data requests and breach notifications >

It requires that organizations take appropriate technical and organizational measures to protect personal data from loss or unauthorized access or disclosure.



GDPR Threads in MS Teams

Especially with external guests

What constitutes personal data?



Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person.

It can be anything from:

- ✓ a name
- ✓ a photo
- ✓ an email address
- ✓ bank details
- ✓ posts on social networking websites
- ✓ medical information
- ✓ computer IP address

Teams and privacy data



Azure and Teams Meetup Germany - January 20... > **Gener...** ...
Public | No classification |

This team has guests

Conversations Files Wiki Azure and Teams Meetup Germ.. +

General

New Upload Get link Open in SharePoint + Add cloud storage

✓	Type	Name	Modified ▾	
		Teilnehmermail Teams Special V2.docx	1/9/18	...
		Speakermail Teams Special.docx	1/9/18	...
		Teilnehmermail Teams Special.docx	1/9/18	...
		AgendaV5.pptx	1/9/18	...
		TrustInTechLogo-Munich.jpg	12/11/17	...

Teams and Guest Access



Search or type a command

test_test_tpoett.onmicro... 8

Activity

Chat

Teams

Meetings

Calls

Files

...

Favorites

- Azure and Teams Meetup ...
- UC (Nierychlo)
- Teams Guest Access Test G...

General

Conditional Access Test Channel

GDPR Compliance

HotSuit

...

Teams Guest Access Test Group

Public | No classification

Members Channels Settings Apps

This team contains users from outside your organization.

Search for members 9 members Add member

Name	Title	Location	Role
Thomas Poett			Owner
chlasel (Guest)			Guest
chlassow (Guest)			Guest
feschust (Guest)			Guest

Teams and other application (integration)



Search or type a command

test_test_tp

Activity

Chat

Favorites

Azure and Teams Meetup ...

UC (Nierychlo)

Teams Guest Access Test Group > HotSuit ★ ...

This team has guests

Conversations Files Wiki +

HotSuite

About X

Save time by managing all of your social media marketing efforts from a single dashboard. With Hootsuite's platform, you get the tools to manage all your social profiles and automatically find and schedule effective social content.

[Learn more](#)

Add a tab

Turn your favorite apps and files into tabs at the top of the channel.

Search

PowerPoint SharePoint Stream Website Wiki Word

All Tabs

Adobe Creative Cloud Adobe Sign Asana Bitbucket Egnyte Empsense Flipgrid

Freehand b... GitHub Haldor Plag... iGlobe CRM... Intercom Jira Cloud LMS365

MeisterTask MindMeister Nearpod Nimble Con... Perfony Pickit Images Polly

POPIn PowerApps Quizlet Sapho Skooler Smartsheet Sociabble

External Guest Access



Do we create a breach if we activate Office 365 Guest Access?

- What data are exposed to Guests
- What can a Guest access

How do we protect Guest from taking information and data?

The security risks with Guest Access



Guests (with an O365 Account)

- If you give full control to an external user, he could share content with other external users
- It's hard to link the email address you sent the invite to and the Microsoft account associated to the user.
- Permission inheritance if you give access to a site or a Group

Anonymous Guests (not in Teams)

- Anonymous guest links can be shared to other people who might be able to view or edit the content.
- Changes cannot be tracked in the document.



Compliance Control in Office 365

Three important protections pathes



Compliance Manager (GDPR compliance)

- Assess
- Monitor
- Report

RMS (Rights Management)

- Classify
- Protect
- Control

Secure Score (Reporting)

- Report
- Check
- Assess

What is Compliance Manager



GDPR

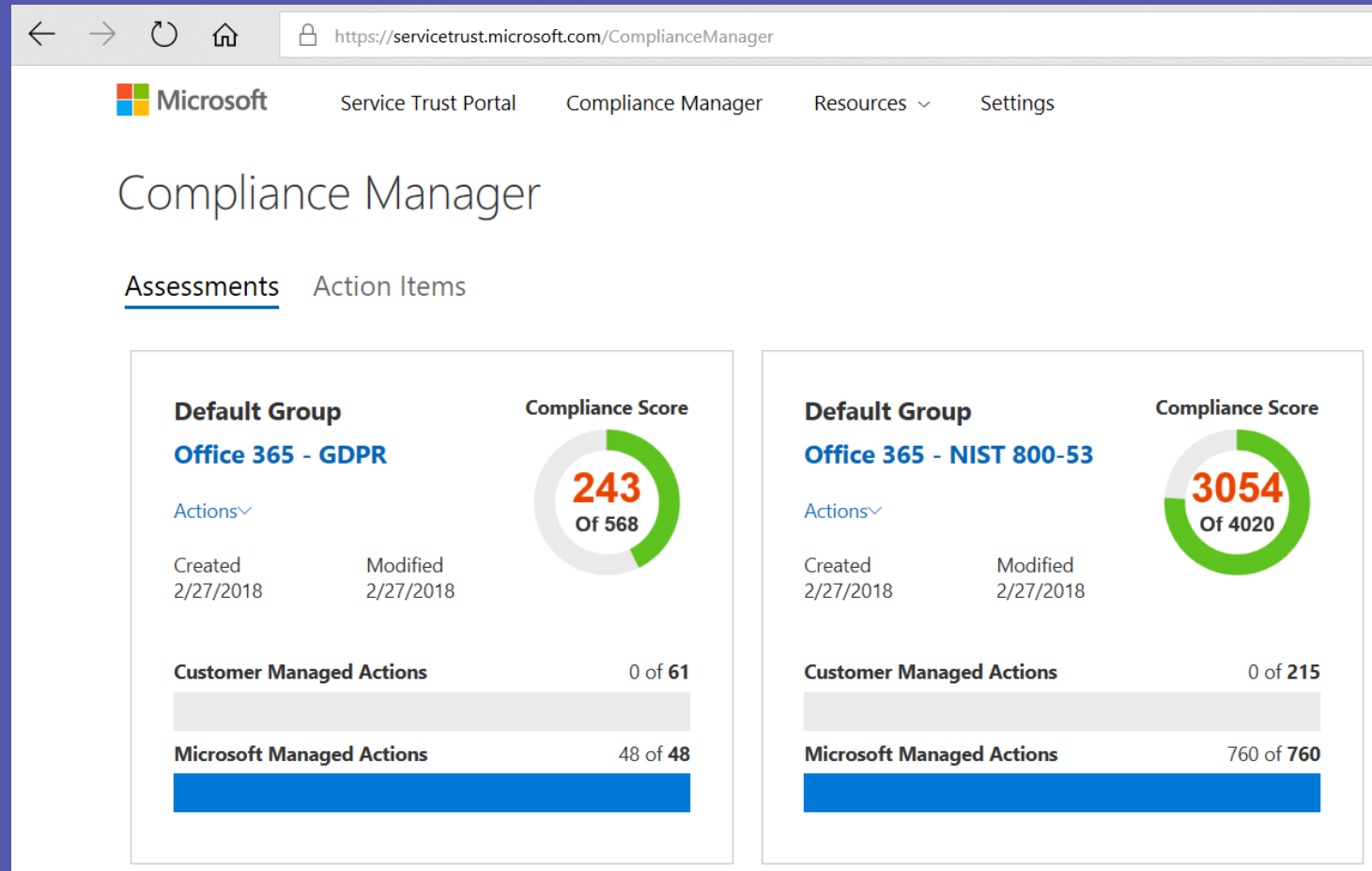
General Data Protection Regulation

DSVGO

DatenSchutz

GrundVerOrdnung

Intelligent scoring that reflects your organization's compliance posture against data protection regulations and standards.



Compliance Manager - Assessment



- Microsoft Task (handled by MSFT)
- Customer Task (handled by YOU)

Browser address: <https://servicetrust.microsoft.com/FrameworkDetailV2/13e69ea7-346c-4bf5-9960-c8bde3c0e4ea>

Microsoft Service Trust Portal Compliance Manager Resources Settings

< Back To Dashboard Export to Excel

Default Group	Office 365	GDPR	48/109	<div style="width: 44%;"></div>	In Progress	27.02.2018	<div style="width: 24%;">243 of 568</div>
Group Name	Product	Assessment	Assessed Controls	44% Assessed	Status	Last Modified	Compliance Score

Rights of individuals 0/6 Assessed ^

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
<p>Control ID: A.7.2.1</p> <p>Title: Determining PII principals' rights and enabling exercise</p> <p>Article ID: Article (12)(2)</p> <p>Description: Article (12)(2): The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject</p>	6	GDPR: A.7.1.2, A.7.1.3, A.7.2.4, A.7.2.5, A.7.2.7, A.7.2.8	<div style="background-color: #0070c0; color: white; padding: 2px 5px; border-radius: 3px;">Assign</div> <div style="margin-top: 5px; font-size: 10pt; color: #0070c0;">Manage Documents</div>	Select v	<div style="border: 1px solid #ccc; padding: 2px; width: 40px; height: 20px; margin: 0 auto;"></div>	<div style="border: 1px solid #ccc; padding: 2px; width: 40px; height: 20px; margin: 0 auto;"></div>	Select v

Anonymous Access



- You can expire a shared link (after period)

Recommendation:

Control and classify data (documents)

Don't allow protected content to be shared with anonymous users

Better use guest access with an authenticated external user (user having an O365 account in another tenant)



Applying GDPR in MS Teams

STEPS to comply and protect



Run at least those activities

- Activate Office 365 Secure Score
- Build a RMS Plan
- Run GDPR Assessment

Additionally consider :

Cloud App Security (ensure no Shadow IT)



[Use audit data](#)

You should consume your audit data either through the audit log search or through the Activity API to a third party security information system at least every week. This data enables a wide range of illicit activity detection and security breach scoping and investigation capabilities. Consuming and reviewing it regularly makes it less likely that an attacker will operate in your tenancy undetected for long periods of time. We found that the last time you reviewed this report was not within the suggested timeframe. If you consume this data, your score will go up 5 points.

Action Category	Data
User Impact	Low
Implementation Cost	Low
Action Score	0/5

Threats

- Account Breach
- Data Exfiltration
- Data Deletion
- Elevation of Privilege
- Malicious Insider

Dashboard

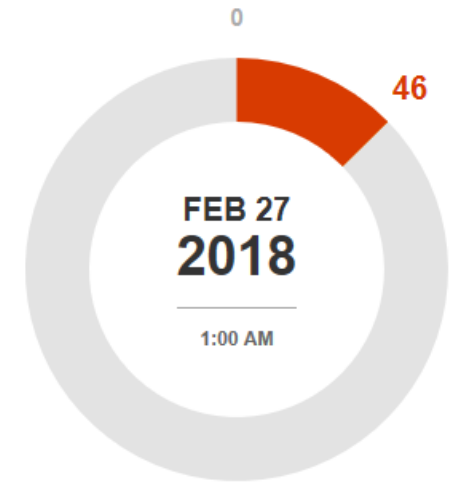
Score Analyzer

Your Secure Score Summary

Your Secure Score is:

46

Of 364



Take action to see how you can improve your score today

For more information about your Secure Score go to: [Score Analyzer](#).

Choosing your activation method (RMS)



NOTE:

- M365 E3/ E5
(Secure Productive Enterprise (SPE))
- or
- Azure Information Protection Premium P1/ P2
- or
- EMS E3/ E5

The screenshot shows two overlapping web portals. The background is the Office 365 'Rights management' page, which includes a green checkmark icon and a 'deactivate' button. The foreground is the Microsoft Azure portal, specifically the 'Azure Information Protection - Global policy' configuration page. The Azure portal interface includes a search bar, a left-hand navigation menu with options like 'Dashboard', 'All resources', and 'Global policy', and a main content area with sections for 'GENERAL', 'POLICIES', and 'MANAGE'. The 'POLICIES' section is active, showing a table for configuring labels.

Configure administrative name, description and scope for this policy			
* Policy name			
<input type="text" value="Global"/>			
Policy description			
<input type="text" value="Default policy for all users in the tenant"/>			
Select which users or groups get this policy. Groups must be email-enabled.			
Configure labels for this policy and order them by sensitivity level			
LABEL DISPLAY NAME	POLICY	MARKING	PROTECTION
Personal	Global		...
Public	Global		...
General	Global		...
Confidential	Global		...
Highly Confidential	Global		...
Protection templates	Global		...

<https://docs.microsoft.com/en-us/information-protection/deploy-use/activate-service>

<https://account.activedirectory.windowsazure.com/RmsOnline/Manage.aspx?brandContextID=O365>

Security & Compliance



Use S&C labeling your data for classification and protect, as well as for compliance and retention.

Home > Labels

When published, labels appear in your users' apps, such as Outlook, SharePoint, and OneDrive. When a label is applied to email or documents, it can be used to protect content, such as labels that retain content for a certain time or ones that simply delete content when it reaches a certain age. [Learn more about labels](#)

[+ Create a label](#) [Publish labels](#) [Auto-apply a label](#) [Refresh](#)

<input type="checkbox"/>	Name	Created by
<input type="checkbox"/>	General PII Informaion (contains)	Thomas Poett (ADMIN)
<input type="checkbox"/>	Personenbezogene Daten Typ 2	Phillip Heinz
<input type="checkbox"/>	Personenbezogene Daten "Typ 1"	Phillip Heinz

Office 365 Cloud App Security

Office 365 Cloud App Security is a subset of Microsoft Cloud App Security that provides enhanced visibility and control for Office 365. This includes threat detection based on user activity logs, discovery of Shadow IT for apps that have similar functionality to Office 365

The screenshot shows the Office 365 Cloud App Security portal interface. The browser address bar displays the URL: `https://tpoett.portal.cloudappsecurity.com/#/services/28375?tab=info`. The navigation bar includes 'Cloud App Security', 'Discover', 'Investigate', 'Control', and 'Alerts'. The main content area is titled 'Microsoft Teams Collaboration' and features a 'Protected app' section for Microsoft Teams. A score of 10 is displayed in a green circle. Below this, there are sections for 'GENERAL', 'SECURITY', and 'COMPLIANCE' with various security and compliance checks marked with green checkmarks.

Protected app			
Microsoft Teams, the new chat-based workspace in Office 365.			Suggest an improvement Disclaimer
10 GENERAL			
Category: Collaboration	Headquarters: United States	Data center: Multiple locations	Hosting company: Microsoft Corporation
Founded: 1975	Holding: Public	Domain: *.teams.microsoft.com	Terms of service: go.microsoft.com/fwlink/?Li...
Domain registration: Jul 9, 2002	Consumer popularity: 10	Privacy policy: go.microsoft.com/fwlink/?Linkl...	Logon URL: login.microsoftonline.com
Vendor: Microsoft	GDPR readiness statement: blogs.microsoft.c...		
10 SECURITY			
Data-at-rest encryption method: AES	Multi-factor authentication	IP address restriction	User audit trail
Admin audit trail	Data audit trail	User can upload data	Data classification
Remember password	User-roles support	File sharing	Valid certificate name
Trusted certificate	Encryption protocol: TLS 1.2	Heartbleed patched	HTTP security headers: Partial
Supports SAML	Protected against DROWN	Penetration Testing	Password policy
9 COMPLIANCE			
	FISMA	GAAP	HIPAA



Bochum




Dresden



Thank you for your participation

Thomas Poett
MVP

Blog: <http://www.uclabs.blog>

 Meetups
www.meetup.com/Trust-in-Tech-Meetup-Munich/
www.meetup.com/Microsoft-Teams-Meetup-Munich/

 @thomaspoett
 <http://www.uclabs.blog>


Thomas.Poett
@trans4mation.de

Thomas.Poett
@uclabs.blog


Microsoft
Most Valuable Professional
MVP since 2012
+ Microsoft SfB Elite Team