



Moving your collaboration to the Cloud?

Patrick Viaene
Modern Workplace Lead
patrickv@microsoft.com

Once upon a time, 10y ago....



Patrick Viaene
Cloud Sales Manager
Microsoft Belgium & Luxembourg

 patrickv@microsoft.com

 [@patrickvia](https://twitter.com/patrickvia)

Once upon a time, 10y ago....



Once upon a time, 10y ago....

Cloud, should I trust it?

Security

Physical security
Electronical security



Availability

Is the Microsoft-datacenter trustworthy?
Am I not too dependent of my internet-connection?



Privacy

Who has access to my data?
Patriot Act



The Office 365 Trust Center

As an Office 365 customer you have entrusted Microsoft to help protect your data. Microsoft values this trust and cares deeply about the privacy and security of your data. Microsoft strives to take a leadership role in industry privacy, security and compliance practices by following these trust principles.

Office 365 Trust Principles

[Your Privacy Matters >](#)
We respect the privacy of your data

[Leadership in Transparency >](#)
You know 'where' data resides, 'who' can access it and 'what' we do with it

[Independently Verified >](#)
Compliance with World Class Industry standards verified by 3rd parties

[Relentless on Security >](#)
Excellence in Cutting edge security practices

A customer has options (and responsibility)

Data retention, deletion, and destruction in Microsoft 365

Article • 11/17/2021 • 2 minutes to read • 1 contributor



Microsoft has a Data Handling Standard policy for Microsoft 365 that specifies how long customer data is retained after deletion. There are generally two scenarios in which customer data is deleted:

- **Active Deletion:** The tenant has an active subscription and a user or administrator deletes data, or administrators delete a user.
- **Passive Deletion:** The tenant subscription ends.

A customer has options (and responsibility) - 2

Where your Microsoft 365 customer data is stored

Article • 04/27/2022 • 176 minutes to read • 10 contributors



The tables below shows where customer data is stored at-rest for Microsoft 365 services across all of Microsoft's global cloud locations. Expand the location of your billing address country to find out where customer data for each service would be stored.

If your business is located in the European Union, see [Data locations for the European Union](#) for more information.

Customers should view tenant specific data location information in your Microsoft 365 admin center in **Settings > Org settings > Organization profile tab** [↗](#) > **Data location**. If you [requested to move to a new Geo](#), the data location information in the Microsoft 365 admin center may show only your new Geo even though some data may be stored temporarily in your prior Geo during the transition.

New Microsoft 365 tenants are defaulted to Geo based on the country of the transaction associated with that tenant's first subscription.

Find information about the contractual commitments for the storage location of customer data at rest in the [Microsoft Products and Services Data Protection Addendum \(DPA\)](#) [↗](#).

Statement

Teams uses SharePoint online as underlying storage, management and collaboration platform

A customer has options (and responsibility) - 3

Manage retention policies for Microsoft Teams

Article • 03/21/2022 • 5 minutes to read • 18 contributors • Applies to: Microsoft Teams



Note

If you are seeing a message in Teams that your chats or messages have been deleted by a retention policy, see [Teams messages about retention policies](#).

The information on this page is for IT administrators who manage these retention policies.

Retention policies and retention labels from Microsoft 365 help you to more effectively manage the information in your organization. You can configure retention settings to keep data that's needed to comply with your organization's internal policies, industry regulations, or legal requirements. You can also configure retention settings to delete data that's considered a liability, that you're no longer required to keep, or that has no legal or business value.

Teams supports retention policies for chat and channel messages so that as an admin, you can decide proactively whether to retain this data, delete it, or retain it for a specific period of time and then delete it. The start of the retention period for these actions is always

Teams recordings

Teams cloud meeting recording


Article • 05/12/2022 • 18 minutes to read • 43 contributors • Applies to: Microsoft Teams



In Microsoft Teams, users can record their Teams meetings and group calls to capture audio, video, and screen sharing activity. There is also an option for recordings to have automatic transcription, so that users can play back meeting recordings with closed captions and review important discussion items in the transcript. The recording happens in the cloud and is saved to Microsoft OneDrive for Business and Microsoft SharePoint Online, so users can share it securely across their organization.

When a meeting is recorded, it's automatically:

- Uploaded to OneDrive for Business or SharePoint Online
- Permissioned to the people invited to the meeting
- Linked in the chat for the meeting
- Displayed in the Recordings and Transcripts tab for the meeting in Teams calendar
- Added to various file lists across Microsoft 365: Shared with me, office.com, Recommended, Recent, etc.
- Indexed for Microsoft 365 Search

Related: [Teams meeting recording end user documentation](#) 



Changes –
in the wake
of *Schrems*
//



New Standard Contractual Clauses: Background

- Schrems II ruling & recommendations from the European Data Protection Board (EDPB):
 - - the SCCs remain a valid transfer mechanism
- Supplementary measures might be needed in addition.
- Microsoft implemented the New SCC on September 15, 2021.
- SCCs offered in conjunction with safeguards of existing supplementary measures



Supplementary Measures implemented by Microsoft

Microsoft views its commitments under the new SCCs, in conjunction with the safeguards Microsoft provides with existing supplementary measures and such additional supplementary measures as the Defending your Data protections, **as helping ensure an adequate level of data protection.**

Microsoft has already implemented several:

- technical,
- organizational, and
- contractual measures

in line with those that the EDPB included in its recommendations.

Microsoft's **Defending Your Data** commitments, for example, fully aligns with the EDPB recommendations. Microsoft continuously evaluates what and when other measures may be appropriate in line with the recommendations.

Contractual commitments

- We do not provide any government with direct and unfettered access
- We do not provide any government with the ability to break encryption.
- Microsoft does comply with applicable law.
-
- Microsoft only responds to requests for specific accounts/identifiers.
- Microsoft does review every legal demand to ensure it is valid

Defending Your Data

Microsoft was the first company to respond to the EDPB's recommendations with new commitments that demonstrate the strength of our conviction to defend our customers' data. These protections are called "Defending Your Data."

First, we are committing that we will challenge every government request for public-sector or enterprise customers' data—from any government—where there is a lawful basis for doing so. This strong commitment goes beyond the proposed recommendations of the European Data Protection Board.

Second, we will provide monetary compensation to these customers' users if we disclose their data in response to a government request in violation of the EU's GDPR. This commitment also exceeds the EDPB's draft recommendations. It shows Microsoft is confident that we will protect our public sector and enterprise customers' data and not expose it to inappropriate disclosure.



For more information, see the ["New Steps to Defend Your Data"](#) blog post.

An EU Data Boundary for the Microsoft Cloud

*Announced on 6 May
2021*



An EU Data Boundary for the Microsoft Cloud

Data storage and processing:

- *For all commercial and public-sector customers located in our new EU Data Boundary, Microsoft will store and process the customers' personal data in the EU Data Boundary by the end of 2022, including diagnostic data, service-generated data and the data Microsoft uses to provide technical support*
- *This strengthens and extends our current commitments around data in transit and at rest*
- *This commitment will apply to each of our three main cloud services – Azure, Microsoft 365 (including Teams and OneDrive for Business) and Dynamics 365 (including Power Platform), as well as associated customer support operations*
- *There may be a small number of instances where a particular additional feature still requires the transfer of data outside the EU Data Boundary. We will provide customers choices over whether to enable those features*

<https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/>

Answering Europe's Call: Storing and Processing EU Data in the EU

May 6, 2021 | [Brad Smith - President and Chief Legal Officer](#)



Today we are announcing a new pledge for the European Union. If you are a commercial or public sector customer in the EU, we will go beyond our existing data storage commitments and enable you to process and store all your data in the EU. In other words, we will not need to move your data outside the EU. This commitment will apply across all of Microsoft's core cloud services – Azure, Microsoft 365, and Dynamics 365. We are beginning work immediately on this added step, and we will complete by the end of next year the implementation of all engineering work needed to execute on it. We're calling this plan the EU Data Boundary for the Microsoft Cloud.

The new step we're taking builds on our already strong portfolio of solutions and commitments that protect our customers' data, and we hope today's update is another step toward responding to customers that want even greater data residency commitments. We will continue to consult with customers and regulators about this plan in the coming months, including adjustments that are needed in unique circumstances like cybersecurity, and we will move forward in a way that is responsive to their feedback.



Microsoft

© Copyright Microsoft Corporation. All rights reserved.