EUROPEAN
COURT
OF AUDITORS

PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about the processing and the protection of your personal data.

Processing operation: ECA M365 environment

Data Controller: ECA.SEC-GEN.SG2 (DIWI)

Record reference: DIWI-417

Contents

1. Introduction

The European Court of Auditors (hereafter 'the Court' or 'the ECA') is committed to protect your personal data and to respect your privacy. The Court collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to the processing operation "ECA M365 environment" undertaken by ECA.SEC-GEN.SG2 is presented below.

M365 is being tested to establish if it can be considered a possible collaborative solution as part of the modernised Digital ECA.

The "Digital ECA" was one of the essential goals defined in ECA's IT Master Plan for 2018-2020" (CA 071/1/17 Rev.1). As part of "Goal 4: Reinventing IT. Towards a digital ECA", it was set forth that "*59. **Cloud services have come to stay** and to reign. Organisations like ECA will not have the means for sustaining fully internally managed IT infrastructures and solutions. **This will be specially the case for common IT services ("commodities") like the email, the Microsoft and collaboration tools, communications services (voice and video telephony, video streaming)** or administrative packages (service management tool, etc.)*" (Heading IT-12 IT infrastructure adapted to the new paradigms: Cloud, Bring Your own Device and consumerisation).

Under the same heading, the document refers to the following initiatives, which directly concern the M365 experimentation: "*62. The following initiatives will contribute to this objective: […]*

- ***Promote the use of "Software as a service" solution for all business areas implementing the "buy before build" principle**.*
- *Use of widely used apps and social networks […] in our professional environment.*"

These decisions were confirmed and further detailed when the following document was formally adopted by the Court: "*State of play of IT Cloud services at the ECA and proposal for the next steps in 2021*" (CA 035/21).

In particular, it confirmed that ECA will: "***make full use of Teams capabilities for collaborative work, entailing integration with other Microsoft 365 services (Sharepoint online and OneDrive)***" (2021 cloud roadmap at the ECA, 9. 40 (2)).

2. Why and how do we process your personal data?

Purpose of the processing operation:

DIWI is operating the future collaboration platform of the European Court of Auditors, providing ECA staff with better real-time communication and collaboration tools, making the "access anywhere/anytime/from any device" paradigm possible. A central piece of this ECA Digital Workplace architecture is based on the cloud-based solution Microsoft 365 ("Microsoft 365 platform") provided by Microsoft. This enables ECA staff to work on any (corporate) device and facilitates collaboration with internal and external stakeholders.

2.1. Description of the processing related to each data category

The Microsoft 365 platform distinguishes between the following data categories as defined in detail in section 4 of this document:

- Customer data (Identification data and content data)
- Service generated data
- Diagnostic data

Any of these categories may contain personal data. The operation of this platform requires the **processing of data categories by Microsoft**, for the following specific purposes:

1. Providing the Microsoft 365 service to the Court
    a. Identification data, content data, service generated data
2. Technical support to IT teams for issues with Microsoft 365
    a. Identification data, service generated data
3. Prevention, detection and resolution of security events (e.g. cyber-attack)
    a. Identification data, service generated data
4. Assistance to data subjects in exercising their rights in relation to data processed within Microsoft 365
    a. Identification data, service generated data

The operation of this platform requires the **processing of data categories by DIWI**, for the following specific purposes:

1. Set-up, configuration and maintenance of Microsoft 365 capabilities
    a. Identification data, service generated data
2. Administration of the rights allocated to a user account
    a. Identification data
3. End-user support for issues with Microsoft 365
    a. Identification data, service generated data
4. Prevention, detection and resolution of security events (e.g. cyber-attack)
    a. Identification data, service generated data
5. Assistance to data subjects in exercising their rights in relation to data processed within Microsoft 365
    a. Identification data, service generated data

The above-mentioned processing of personal data by DIWI and/or Microsoft is done to provide the cloud component of the ECA Digital Workplace services.

2.2. For the EU Institutions, Bodies and Agencies, Microsoft processes also your personal data for the finite set of processing for Microsoft's business operations that are incident to delivery of the online services as data processor (exhaustive list):

1. Billing and Account Management
    a. Identification data, service generated data
2. Compensation
    a. Service generated data
3. Internal Reporting and Business Modelling
    a. Service generated data
4. Combatting fraud, Cybercrime, and Cyberattacks
    a. Identification data, service generated data
5. Improving Core Functionality of Accessibility, Privacy and Energy Efficiency
    a. Service generated data
6. Mandatory Financial Reporting and Compliance with Legal Obligations
    a. Identification data, service generated data

Your personal data will not be used for an automated decision-making including profiling, advertising or marketing.

The Data Controller reserves the right to consult user activity based on service generated data to maintain the security and integrity of the ECA M365 environment.

3. On what legal ground(s) do we process your personal data?

Article 5.1 (a) of the Regulation 2018/1725 states that: "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body*.". This legal basis shall be laid down in Union Law (Article 5.2 Regulation (EU) 2018/1725).

According to the Articles 285, 286 and 287 of the Treaty on the Functioning of the European Union (TFEU):

- The ECA examines the accounts of all revenue and expenditure of the Union and also examines the accounts of all revenue and expenditure of all bodies, offices or agencies set up by the Union, in so far as the relevant constituent instrument does not preclude such examination.
- The ECA provides the European Parliament and the Council with a statement of assurance as to the reliability of the accounts and the legality and regularity of the underlying transactions, which is published in the Official Journal of the European Union. This statement may be supplemented by specific assessments for each major area of Union activity.
- The ECA examines whether all revenue has been received and all expenditure incurred in a lawful and regular manner and whether the financial management has been sound. In doing so, the Court has to report in particular on any cases of irregularity.

In addition, the processing of personal data can also be carried out for the performance of tasks carried out in the public interest by the Union institutions and bodies that is

necessary for the management and functioning of those institutions and bodies. All personal data connected to the use of Microsoft 365 are processed based on the necessity for the performance of a task carried out in the public interest by the ECA, including the processing of personal data that are necessary for the management and functioning of the ECA.

More specifically, the objective of all processing activities related to Microsoft 365 is to support the management and the functioning of the European Court of Auditors, by:

- adjusting the internal mechanisms and management systems to the new technological environment and advancements,
- providing to ECA members of the personnel the necessary means and tools to perform their daily tasks, and by
- organizing ECA's operations according to the principles of sound financial management, encoded in Article 33 of the Regulation 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012.

The digital transformation of the ECA is in line with the in ECA's IT Master Plan for 2018-2020" (CA 071/1/17 Rev.1), and Secretariat-General 2021-2025 Strategy Development Plan for our People, Workplace and Services (CA 037/21 FINAL).

These actions will be guided by the following detailed strategy as adopted by the Court: State of play of IT Cloud services at the ECA and proposal for the next steps in 2021 (CA 035/21).

The deployment of Microsoft 365 cloud services makes part of the implementation of the Secretariat-General 2021-2025 Strategy Development Plan.

4. Which personal data do we collect and further process?

DIWI and Microsoft process four different categories of data related to the provision of the service, all of which may include personal data. These categories are:

1. Identification data which contains personal data necessary for the identification of the user and the corresponding user account, such as:
   - ECA username, email address and account status.
   - User personal data (title, last name, first name, nationality)
   - Function-related data (employee ID, administrative entity and grade, office address and telephone number, city and country)

   Note that identification data is visible to everyone having access to the ECA M365 environment.
2. Content data includes any content uploaded to the Microsoft 365 platform by its users, such as documents, and multimedia (e.g. video recordings). Such data is stored by the user in Microsoft 365, but not otherwise processed by the service.

3. Diagnostic data (also known as telemetry data) is related to the data subjects' usage of Microsoft client software. DIWI has applied technical measures to disable sharing of diagnostic data with external parties, including with Microsoft.
4. Service generated data contains information related to the data subjects' usage of online services, most notably the user IP address, creation time, site URL and user email address. This data is generated by events that are related to user activity in Microsoft 365. This data from online services is used to make sure performance, security and scaling are appropriate. To learn which events trigger the creation of service generated data, consult Annex A.

There might be personal information being processed, in particular personal information contained within the content data of individual users or groups of users in each service within the European Court of Auditors, in addition to the personal data processed by all M365 tools that are covered by this privacy statement. This refers, for example, to documents or messages exchanged between members of a specific group or team.

The decision what data should be processed using M365 remains fully with the respective operational controller or user. Separate policies or instructions concerning this data may exist and need to be taken into account. Relevant documents might for instance be:

- instructions, policy and procedure about how to process HR-related data (e.g. Teams shall be not be used to provide information to staff about the staff financial rights),
- Instructions, policy and procedure about how to process medical data (e.g. using dedicated channels and means of communication to share medical certificates with the ECA Medical service),
- Instructions, policy and procedure about how to process audit data, EU classified information, and otherwise, any other category of data.

DIWI does not take responsibility for the inappropriate use of M365. Please refer to the relevant record and privacy statement of the particular processing activity for further information.

DIWI and Microsoft do NOT process special categories of personal data in the context of Microsoft 365. Nevertheless, end-users and services may use Microsoft365 as a means for processing special categories of personal data in the context of specific policies.

5. How long do we keep your personal data?

ECA.SEC-GEN.SG2 only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing.

- Identification data
    - for as long as the user account is active plus 30 days after the account's deletion
- Content data

    - Between 90 and 180 days upon expiration/termination of the subscription for services with Microsoft. Notwithstanding, the operational controller and/or user can erase the content under their control at any time or following a defined retention schedule applicable to the content in question.
- Service generated data
    - Automatic deletion at most 180 days after expiration/termination of the subscription for services with Microsoft.
- Diagnostic data
    - Automatic deletion at most 180 days after expiration/termination of the subscription for services with Microsoft.

6. How do we protect and safeguard your personal data?

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the European Court of Auditors' Data Centre, or in Microsoft datacentres in the EU (linked to the Court's Microsoft 365 environment).

In order to protect your personal data, the Court has put in place several strong contractual safeguards, complemented by technical and organisational measures. In addition to the general policy of Microsoft to secure personal data by means of pseudonymisation and encryption, the risk of disclosure of personal data to third country authorities by Microsoft Ireland and its affiliates is mitigated by customized contractual provisions, which address the way Microsoft responds to access requests, limiting risks to personal data of the ECA users of the services. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

If users access the Microsoft 365 service from outside the EU/EEA, personal data may be transferred to a corresponding location in order to provide the service.

Any data in transit is protected by strong encryption.

7. Who has access to your personal data and to whom is it disclosed?

Access to your personal data is provided to the Court staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements. Those members of staff include appointed ECA officials and external contractors under the supervision of the abovementioned officials. The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

For services related to the Microsoft 365 cloud-based collaboration platform, Microsoft acts as data processor. Contact details: Microsoft Ireland, South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland.

8. What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access your personal data and to rectify them in case your personal data are inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing, and the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a) on grounds relating to your particular situation.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address to the European Data Protection Supervisor. Their contact information is given under "Contact information" Section 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description in your request.

In the context of Microsoft 365, the "User data search" helps the Data Controller retrieve personal data upon data subject request.

9. Contact information

The Data Controller:

> If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, ECA.SEC-GEN.SG2 at eca-howcanwehelp@eca.europa.eu.

The Data Protection Officer (DPO) of the Court:

> You may contact the ECA's Data Protection Officer at ECA-Data-Protection@eca.europa.eu or by mail at any time if you have any concerns and/or complaints about the processing of your personal data.
>
> European Court of Auditors
> Data Protection Officer
> 12 rue Alcide de Gasperi
> 1615 Luxembourg
> LUXEMBOURG

The European Data Protection Supervisor (EDPS):

> You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider

that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

10. Where to find more detailed information?

The Court Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Court, which have been documented and notified to him. You may access the register here.

This specific processing operation has been notified to the DPO who provided the Record reference number DIWI-417, and will soon be included in the DPO's public register.

24 September 2021

****

Annex A – Examples of user activity events that create service generated data

Personal data might be processed through logs for the purposes that are referred to in Section 2.1. in an exhaustive manner.

SharePoint Online and OneDrive for Business

File and page activities

Short	Description
Accessed file	User accesses a file.
Extended accessed file	An event is logged when the same user continually accesses a file for an extended period (up to 3 hours).
Changed retention label for a file	A retention label was applied to or removed from a document.
Changed record status to locked	The record status of a retention label that classifies a document as a record was locked.
Changed record status to unlocked	The record status of a retention label that classifies a document as a record was unlocked.
Checked in file	User checks in a document that they checked out from a document library.
Checked out file	User checks out a document located in a document library.
Copied file	User copies a document from a site.
Deleted file	User deletes a document from a site.
Deleted file from recycle bin	User deletes a file from the recycle bin of a site.
Deleted file from secondstage recycle bin	User deletes a file from the second stage recycle bin of a site.
Deleted file marked as a record	A document or email that was marked as a record was deleted.
Detected document sensitivity mismatch	User uploads a document to a site protected with a sensitivity label.
Discarded file checkout	User discards or undoes a checked-out file.
Downloaded file	User downloads a document from a site.
Modified file	User modifies the content or the properties of a document on a site.
Moved file	User moves a document from its current location on a site to a new location.
Previewed file	User previews files on a site.
Performed search query	User performs a search.
Recycled all minor versions of file	User deletes all minor versions from the version history of a file.
Recycled all versions of file	User deletes all versions from the version history of a file.

Recycled version of file	User deletes a version from the version history of a file.
Renamed file	User renames a document on a site.
Restored file	User restores a document from the recycle bin of a site.
Uploaded file	User uploads a document to a folder on a site.
Viewed page	User views a page on a site.
View signalled by client	The indicated page has been viewed by the user.

Folder activities

Short	Description
Copied folder	User copies a folder from a site to another location.
Created folder	User creates a folder on a site.
Deleted folder	User deletes a folder from a site.
Deleted folder from recycle bin	User deletes a folder from the recycle bin on a site.
Deleted folder from second-stage recycle bin	User deletes a folder from the second-stage recycle bin on a site.
Modified folder	User modifies a folder on a site.
Moved folder	User moves a folder to a different location on a site.
Renamed folder	User renames a folder on a site.
Restored folder	User restores a deleted folder from the recycle bin on a site.

SharePoint list activities

Short	Description
Created list	User created a SharePoint list.
Created list column	User created a SharePoint list column.
Created list content type	User created a list content type.
Created list item	User created an item in an existing SharePoint list.
Created site column	User created a SharePoint site column.
Created site content type	User created a site content type.
Deleted list	User deleted a SharePoint list.
Deleted list column	User deleted a SharePoint list column.
Deleted list content type	User deleted a list content type.
Deleted list item	User deleted a SharePoint list item.
Deleted site column	User deleted a SharePoint site column.
Deleted site content type	User deleted a site content type.
Recycled list item	User moved a SharePoint list item to the Recycle Bin.
Restored list	User restored a SharePoint list from the Recycle Bin.
Restored list item	User restored a SharePoint list item from the Recycle Bin.

Updated list	User updated a SharePoint list by modifying one or more properties.
Updated list column	User updated a SharePoint list column by modifying one or more properties.
Updated list content type	User updated a list content type by modifying one or more properties.
Updated list item	User updated a SharePoint list item by modifying one or more properties.
Updated site column	User updated a SharePoint site column by modifying one or more properties.
Updated site content type	User updated a site content type by modifying one or more properties.

Sharing and access request activities

Short	Description
Added permission level to site collection	A permission level was added to a site collection.
Accepted access request	An access request to a site, folder, or document was accepted.
Accepted sharing invitation	User accepted a sharing invitation.
Blocked sharing invitation	A sharing invitation sent by a user is blocked due to an external sharing policy.
Created access request	User requests access to a site, folder, or document they do not have permissions to access.
Created a company shareable link	User created a company-wide link to a resource.
Created an anonymous link	User created an anonymous link to a resource.
Created secure link	A secure sharing link was created to this item.
Created sharing invitation	User shared a resource with a user who is not in the directory.
Deleted secure link	A secure sharing link was deleted.
Denied access request	An access request to a site, folder, or document was denied.
Removed a company shareable link	User removed a company-wide link to a resource.
Shared file, folder, or site	User shared a file, folder, or site with a user in the directory.
Updated access request	An access request to an item was updated.
Updated sharing invitation	An external sharing invitation was updated.
Unshared file, folder, or site	User unshared a file, folder, or site that was previously shared.
Used a company shareable link	User accessed a resource by using a link accessible to all users in the organisation.
Used secure link	User used a secure link.

User added to secure link	User was added to the list of entities who can use a secure sharing link.
User removed from secure link	User was removed from the list of entities who can use a secure sharing link.
Withdrew sharing invitation	User withdrew a sharing invitation to a resource.

Synchronization activities

Short	Description
Allowed computer to sync files	User successfully establishes a sync relationship with a site.
Blocked computer from syncing files	User tries to establish a sync relationship with a site from a computer that does not belong to the domain.
Downloaded files to computer	User establishes a sync relationship and successfully downloads files for the first time to their computer from a document library.
Downloaded file changes to computer	User successfully downloads any changes to files from a document library.
Uploaded files to document library	User establishes a sync relationship and successfully uploads files for the first time from their computer to a document library.
Uploaded file changes to document library	User successfully uploads changes to files on a document library.

Site permissions activities

Short	Description
Added site collection admin	Site collection administrator or owner adds a user as a site collection administrator for a site.
Added user or group to SharePoint group	User added a member or guest.
Broke permission level inheritance	An item was changed so that it no longer inherits permissions from its parent.
Broke sharing inheritance	An item was changed so that it no longer inherits sharing permissions from its parent.
Created group	Site administrator or owner creates a group for a site or performs a task that results in a group being created.
Deleted group	User deletes a group from a site.
Modified access request setting	The access request settings were modified on a site.
Modified 'Members Can Share' setting	The Members Can Share setting was modified on a site.
Modified permission level on a site collection	A permission level was changed on a site collection.

Modified site permissions	Site administrator or owner changes the permission level that is assigned to a group on a site.
Removed permission level from site collection	A permission level was removed from a site collection.
Removed site collection admin	Site collection administrator or owner removes a user as a site collection administrator for a site.
Removed user or group from SharePoint group	User removed a member or guest.
Requested site admin permissions	User requests to be added as a site collection administrator for a site collection.
Restored sharing inheritance	A change was made so that an item inherits sharing permissions from its parent.
Updated group	Site administrator or owner changes the settings of a group for a site.

Site administration activities

Short	Description
Allowed user to create groups	Site administrator or owner adds a permission level to a site that allows users assigned that permission to create a group for that site.
Deleted site	Site administrator deletes a site.
Enabled document preview	Site administrator enables document preview for a site.
Enabled legacy workflow	Site administrator or owner adds a Legacy Workflow content type to the site.
Enabled result source for People Searches	Site administrator creates the result source for People Searches for a site.
Enabled RSS feeds	Site administrator or owner enables RSS feeds for a site.
Joined site to hub site	A site owner associates their site with a hub site.
Renamed site	Site administrator or owner renames a site
Unjoined site from hub site	A site owner disassociates their site from a hub site.

Microsoft Teams activities

Short	Description
Added bot to team	User adds a bot to a team.
Added channel	User adds a channel to a team.
Added connector	User adds a connector to a channel.
Added members	A team owner adds members to a team, channel, or group chat.
Added tab	User adds a tab to a channel.
Changed channel setting	Changes name or description of a team channel.
Changed role of members	A team owner changes the role of members in a team.
Changed team setting	User changes the access type, information classification, name, team description of a team or made changes to team settings.
Created team	User creates a team.
Deleted channel	User deletes a channel from a team.
Deleted team	A team owner deletes a team.
Installed app	An app was installed.
Performed action on card	User took action on an adaptive card within a chat.
Removed bot from team	User removes a bot from a team.
Removed connector	User removes a connector from a channel.
Removed members	A team owner removes members from a team, channel, or group chat.
Removed tab	User removes a tab from a channel.
Uninstalled app	An app was uninstalled.
Updated connector	User modified a connector in a channel.
Updated tab	User modified a tab in a channel.
User signed in to Teams	User signs into a Microsoft Teams client.

Microsoft Teams Shifts activities

Short	Description
Added scheduling group	User successfully adds a new scheduling group to the schedule.
Edited scheduling group	User successfully edits a scheduling group.
Deleted scheduling group	User successfully deletes a scheduling group from the schedule.
Withdrew schedule	User successfully withdraws a published schedule.
Added shift	User successfully adds a shift.
Edited shift	User successfully edits a shift.
Deleted shift	User successfully deletes a shift.
Added time off	User successfully adds time off on the schedule.
Edited time off	User successfully edits time off.

Deleted time off	User successfully deletes time off.
Added open shift	User successfully adds an open shift to a scheduling group.
Edited open shift	User successfully edits an open shift in a scheduling group.
Deleted open shift	User successfully deletes an open shift from a scheduling group.
Shared schedule	User successfully shared a team schedule for a date range.
Clocked in using Time clock	User successfully clocks in using Time clock.
Clocked out using Time clock	User successfully clocks out using Time clock.
Started break using Time clock	User successfully starts a break during an active Time clock session.
Ended break using Time clock	User successfully ends a break during an active Time clock session.
Added Time clock entry	User successfully adds a new manual Time clock entry on Time Sheet.
Edited Time clock entry	User successfully edits a Time clock entry on Time Sheet.
Deleted Time clock entry	User successfully deletes a Time clock entry on Time Sheet.
Added shift request	User added a shift request.
Responded to shift request	User responded to a shift request.
Canceled shift request	User cancelled a shift request.
Changed schedule setting	User changes a setting in Shifts settings.
Accepted off shift message	User acknowledges the off-shift message to access Teams after shift hours.

Microsoft Forms activities

Short	Description
Created comment	Form owner adds comment or score to a quiz.
Created form	Form owner creates a new form.
Edited form	Form owner edits a form such, as creating, removing, or editing a question.
Moved form	Form owner moves a form.
Deleted form	Form owner deletes a form.
Viewed form (design time)	Form owner opens an existing form for editing.
Previewed form	Form owner previews a form.
Exported form	Form owner exports results to Excel.
Allowed share form for copy	Form owner creates a template link to share the form with other users.
Disallowed share form for copy	Form owner deletes template link.

Added form co-author	User uses a collaboration link to help design or view responses.
Removed form co-author	Form owner deletes a collaboration link.
Viewed response page	User has opened a response page to view.
Created response	User has submitted a response to a form.
Updated response	Form owner has updated a comment or score on a quiz.
Deleted all responses	Form owner deletes all response data.
Deleted Response	Form owner deletes one response.
Viewed responses	Form owner views the aggregated list of responses.
Viewed response	Form owner views a particular response.
Created summary link	Form owner creates summary results link to share results.
Deleted summary link	Form owner deletes summary results link.
Updated form phishing status	This event is logged whenever the detailed value for the internal security status was changed.
Updated user phishing status	This event is logged whenever the value for the user security status was changed.
Sent Forms Pro invitation	User clicks to activate a Pro trial.
Updated form setting	Form owner updates a form setting.
Updated user setting	Form owner updates User setting.
Listed forms	Form owner is viewing a list of forms.
Submitted response	User submits a response to a form.

Forms activities performed by co-authors and anonymous responders

Activity type	Internal or external user	Organization logged in to	Forms user type
Co-authoring activities	Internal	Form owner's org	Co-author
Co-authoring activities	External	Co-author’s org	Co-author
Co-authoring activities	External	Form owner's org	Co-author
Response activities	External	Responder's org	Responder
Response activities	External	Form owner's org	Responder
Response activities	Anonymous	Form owner's org	Responder

Actions logged in Stream

Note that the content of Stream videos is not covered with this privacy statement.

Action Name	Definition
Created video	Video entity has been created. No video uploaded yet.
Edited video	Video metadata has been edited.
Deleted video	Video has been deleted.

Uploaded video	Video has been uploaded.
Action Name	Definition
Downloaded video	Video download happened.
Edited video permission	Video permissions were modified
Viewed video	A video has been viewed either in the Stream portal or via embed
Shared video	Video shared via email.
Liked video	A user in the organization liked this video
Unliked video	A user disliked a video which he/she previously liked
Commented on video	A comment was made on a video
Deleted video comment	A comment on a video was deleted
Uploaded text track	A subtitle file was uploaded for a video
Deleted text track	A subtitle file was deleted for a video
Uploaded thumbnail	A custom thumbnail was uploaded for a video
Deleted thumbnail	Custom thumbnail was deleted for a video
Linked on Video	A video was associated with a M365 Group
Created group	An M365 Group was created from Microsoft Stream
Edited group	Metadata was updated for an M365 Group
Deleted group	An M365 Group was deleted from Microsoft Stream
Edited group memberships	M365 Group permissions were edited
Created channel	A new channel was created
Edited channel	Channel metadata was edited
Deleted channel	Channel was deleted
Set channel thumbnail	Logged after thumbnails complete upload
Logon	User Logged in to Microsoft Stream
Edited user settings	User edited user settings such as language

M365 meetings logged data categories

Short	Description
creationDateTime	The meeting creation time in UTC.
lastModifiedDateTime	UTC time when the call record was created.
startDateTime	UTC time when the first user joined the call.
endDateTime	UTC time when the last user left the call.
id	Unique identifier for the call record or session.
joinWebUrl	Meeting URL associated to the call.
type	Indicates the type of the call, e.g. groupCall, peerToPeer.

modalities	List of all the modalities used in the call, e.g. audio, video, screenSharing.
subject	The subject of the online meeting.
organizer	The organizing party's identity: user display name and unique id.
participants	List of distinct identities involved in the call or associated with the online meeting: user display name and unique id.
caller	Endpoint that initiated the session, e.g. user's device, an application.
callee	Endpoint that answered the session, e.g. user's device, an application.
chatInfo	The chat information associated with an online meeting: • unique identifier of a message in a Microsoft Teams channel. • ID of the reply message. • unique identifier for a thread in Microsoft Teams.
videoTeleconferenceId	The video teleconferencing ID.
isEntryExitAnnounced	Whether or not to announce when callers join or leave.
lobbyBypassSettings	Specifies which participants can bypass the meeting lobby.
allowedPresenters	Specifies who can be a presenter in a meeting: • Everyone is a presenter (This is default option). • Everyone in organizer's organization is a presenter. • Only the participants whose role is presenter are presenters. • Only the organizer is a presenter.
userid	The user object id.
availability	The base presence information for a user, e.g. Available, Away, BeRightBack, Busy, DoNotDisturb, Offline, PresenceUnknown.
activity	The supplemental information to a user's availability, e.g. InACall, InAConferenceCall, Inactive,InAMeeting, OffWork, OutOfMicrosoft, Presenting, UrgentInterruptionsOnly.