DPIA on Microsoft Teams, OneDrive Sharepoint and Azure AD (June 2021)

Data protection impact assessment on the processing of Diagnostic Data

Version 1.1

Date	16 February 2022
Status	Public version

Colophon

DPIA by

Ministry of Justice and Security, Strategic Vendor Management Microsoft, Google and AWS (SLM Rijk) and SURF (IT procurement for Dutch universities)
Turfmarkt 147
2511 DP The Hague
PO Box 20301
2500 EH The Hague
www.rijksoverheid.nl/jenv

Contact

Henrique Barnard
E h.m.barnard@minjenv.nl
T 070 370 79 11

Project name

DPIA report Diagnostic Data processing in Microsoft Teams, OneDrive, SharePoint and Azure AD

Appendix

Results technical analysis Diagnostic Data

Authors

Privacy Company
Sjoera Nas and Floor Terra, senior advisors
www.privacycompany.eu

Change log

Version	Date	Summary of input
0.1	31 May 2021	First completed draft with Appendix 1
0.2	10 June 2021	Input Microsoft processed on second technical verification report sent on 8 April 2021, clarifications added after discussions with SLM Rijk and SURF
0.3	24 August 2021	Input Microsoft processed; and a new question addressed about Azure AD with track changes
0.4	10 December	Input Microsoft 2 of 4 issues
0.5	23 December	Input Microsoft 2 of 4 issues
0.6	30 January 2022	Input processed in track changes compared to version 0.2
0.7	30 January 2022	Clean version
0.8	5 February 2022	Input SLM and Microsoft
0.9	8 February 2022	Some corrections and new information added
1.0	14 February 2022	More input Microsoft processed, DTIA completed
1.1	16 February 2022	Public version

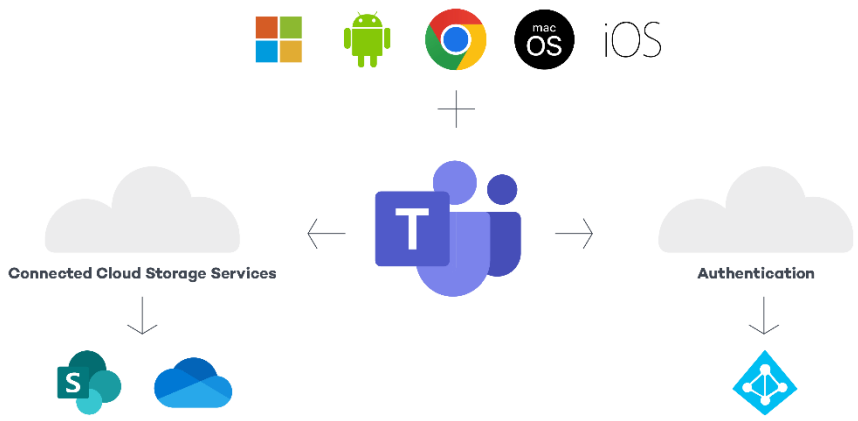
Contents

Summary

This Data Protection Impact Assessment (DPIA) assesses the data protection risks of the (professional) use of Microsoft Teams in combination with OneDrive, SharePoint Online and the Azure Active Directory.

Teams is an online tool for videoconferencing, calling and sharing files. As part of Office 365 Microsoft offers two cloud storage tools for end users: OneDrive and SharePoint Online. These applications are commonly used to access and store files shared via Teams. As a precondition to use Microsoft's online services, end users and admins, including guest users, must be authenticated through the online cloud service Azure Active Directory.

Scope of DPIA
The data processing via Teams and the three cloud services was tested on three different versions of the Office software included in the Microsoft 365 Enterprise license. Teams, SharePoint and OneDrive can be installed on the computers and laptops of employees (Office 365 ProPlus), installed on smartphones and tablets (mobile Office apps for iOS and Android) and as online applications running in a browser (Office for the Web, previously known as Office Online).



This DPIA is a repeated assessment of the use of Teams, SharePoint and OneDrive on two versions of the Office software: Office for the Web and the mobile Office apps. This DPIA contains outcomes with respect to Diagnostic Data processing in Office for the Web and the mobile Office apps as of 31 May 2020, as retested in September 2021.

This DPIA was conducted by SLM Rijk, the central negotiator for Microsoft, Google and Amazon Web Service products and services for Dutch central government organisations and by SURF, the central IT procurement organisation for Dutch universities.

Outcome: six low data protection risks
The outcome of this DPIA, after repeat consultation with Microsoft, is that there are no more known high risks for the Diagnostic Data processing. However, there is a high risk if organisations use Microsoft Teams to process very sensitive and special categories of data, due to the possible access by law enforcement and security services in the USA.

Six low risks related to Diagnostic Data

The six low data protection risks are due to the following circumstances:

1. The current structural **transfer of limited Diagnostic Data and the incidental transfer of security data to the USA** both pose data protection risks. However, these risks can be accepted, as these risks will be mitigated by the end of 2022 the latest, after completion of Microsoft's EU Data Boundary. This means that all Content Data, the Diagnostic Data, as well as the Account Data and the Support Data from EU Enterprise and Education customers will exclusively be processed in Microsoft's EU data centres. Though Microsoft will still transfer some personal data to the USA, to detect and solve security incidents, these ongoing transfers will be incidental, not structural, and they generally only involve pseudonymised and aggregated data.
2. Microsoft is **not very transparent about the browser-based collection of telemetry data** and the telemetry events about the use of the connected experiences. Microsoft calls these diagnostic data *Required Service Data*. Even if a customer has minimised the Office telemetry data collection, by selecting 'neither', this setting does not influence the collection of *Required Service Data*. According to Microsoft, these data are too dynamic or confidential in nature to publish in detail, but Microsoft promises to only process these data for the three agreed processor purposes.
3. Microsoft has committed to improve the take-out tool for the Diagnostic Data, to assist administrators with any **data subject access requests** from individual employees. This tool is currently still difficult to use.
4. There is **one exception** on Microsoft's guarantee that the *Required Service Data* **do not contain directly identifiable (readable) usernames/mail addresses or document names**. As evidenced by the technical network traffic analysis performed for this DPIA, Microsoft can collect the username and/or email address of an employee, together with the tenant's name and the file path with the full name of the document. Microsoft has explained why this can be necessary in OneDrive, for example in case multiple users simultaneously access the same document. Microsoft has also explained that access to these OneDrive diagnostic data is audited, limited to the just-in-time security group, and limited to engineers that have an approved business justification. Additionally, none of these data are retained longer than 30 days.
5. Microsoft offers **two distinct analytics services for Teams**: Teams Analytics & reports and Viva Insights. The first tool (Teams Analytics & reports) provides detailed insights to admins about individual working behaviour. Though Microsoft offers a possibility to pseudonymise the names of the employees, it is not clear if this has any effect on Microsoft's raw data logs. Experienced admins of universities and government organisations can mitigate this risk themselves, by disabling this functionality. Microsoft is not willing to change this default setting. The other tool, Viva Insights is configured disabled by default. This tool includes MyAnalytics and Workplace Analytics, tools that respectively offer employees information about their productivity, and offer managers insights in individual employee work patterns. If an administrator explicitly enables the service, the individual user still has the option to opt-out.
6. Microsoft is in the process of **structurally eliminating traffic to its search engine Bing from SharePoint** when an Enterprise or Education customer has disabled the Controller Connected Experiences. During the initial testing for this DPIA in May 2021, SharePoint sent image queries to Bing when accessed in the browser. As Microsoft is a data controller for Bing, Microsoft permits itself to process personal data for all 17 purposes mentioned in its

general privacy statement. The removal of traffic to Bing from SharePoint should be completed by July 2022.

High risk related to unencrypted streaming and stored special categories of data
There is a high data protection risk related to the possible access by US law enforcement and secret services to very sensitive and special categories of personal data. This risk occurs even though the Teams, OneDrive and SharePoint Content Data are already exclusively processed and stored in the EU, because access to these data can be ordered through US legislation such as the US CLOUD Act. Organisations can mitigate this high risk for OneDrive and SharePoint by using their own encryption keys, with Microsoft Double Key Encryption. Microsoft does not yet offer end-to-end encryption for the streaming communication with multiple participants in Teams, only for unscheduled one-to-one video calls. Though Microsoft has confirmed in reply to this DPIA it will support E2EE in Teams group meetings and chat, it does not yet provide a deadline.

For 'regular' types of personal data, the transfer risks are assessed as very low, even though the possible impact on data subjects can be very high. The chance that Microsoft is compelled to disclose personal data from EU public sector customers is very slim. Though Microsoft cannot disclose if it has **received** any specific legal demands subject to a secrecy obligation. Microsoft publicly explains: "*Microsoft does **not provide**, and has never **provided**, EU public sector customer's personal data to any government.*" This historical fact, combined with the use of the encryption applied by Microsoft, its legal guarantees of contesting each order, its proven track record and its transparency reports, are sufficient to qualify the risk of undue access to the 'regular' personal data as a low data protection risk. However, organisations should not exchange very sensitive or special categories of personal data via Teams, unless the data are publicly available by nature (such as university lectures or some court cases), because they are not in control of the encryption keys.

Scope: Content, Diagnostic and Account Data
This report primarily addresses the data protection risks of the storing by Microsoft of data about the individual use of Teams, OneDrive and SharePoint, in combination with the use of the Azure AD, on all available platforms. These metadata (about the use of the services and software) are called 'Diagnostic Data' in this report.

Technically, Microsoft collects Diagnostic Data in different ways, via system-generated event logs on its own cloud servers and via the telemetry clients in the different clients and through the browser. Similar to the telemetry client in Windows 10 and in Office 365 ProPlus, Microsoft has programmed the mobile Office apps and Office for the Web to systematically collect Telemetry Data on the device, and regularly send these to Microsoft's servers in the USA. Additionally, Microsoft creates detailed Analytics & reports about individual use of Teams.

The scope of this DPIA includes the processing of Content and Account Data, with a focus on the risks of transfer to the USA.

Technical analysis personal data
The technical investigation of the data processing was conducted by running a large number of scripted scenarios and intercepting and analysing the outgoing network traffic, by filing Data Subject Access Requests through a tool Microsoft makes available for admins, and by accessing the individual Teams, SharePoint and OneDrive usage data.

Contents telemetry traffic

The study shows that Microsoft **collects limited data about the individual use of Teams, SharePoint and OneDrive** through the telemetry events. Though the Telemetry Data contain unique UserIDs, device IDs and correlation IDs, the contents are scrambled. However, the technical analysis shows that Microsoft does not comply with its commitment to never include usernames at the (lowest) telemetry level of 'Neither'. **Some telemetry events contained the (readable) user's name in Sharepoint URLs** in the events generated by Teams, OneDrive and SharePoint for the Web (accessed through a browser) and in OneDrive on iOS. According to Microsoft's response to this DPIA, the collection of these content data/directly identifiable data, in combination with the pseudonymised user identifier, is strictly necessary for limited bug detection.

Except for these directly identifiable usernames and OneDrive pathnames, Privacy Company did not observe any Content Data in the intercepted telemetry events. The events also did not contain information about file names or other user supplied data such as device or profile names.

Contents log files cloud servers

The audit log files, and the automated access requests (DSARs) show that Microsoft processes directly identifiable personal data in its Diagnostic Data about the use of Teams, OneDrive and SharePoint in combination with the Azure AD. The log files about the test users demonstrate that a directly identifiable person performed an action at a specific time in a tested app, with which browser and from which operating system. Microsoft also records whether there was a login error, what the cause was, and how the user was authenticated. The users are directly identifiable by the fields with the username and the email address. These access files also contain the used IP address. Because each log line contains the combination of UserId and Organisation ID, each log line is personal data. In addition, these log files contain information about actions on the servers, and Content Data from names of paths and files.

Purposes, roles and legal grounds

The privacy amendment negotiated by SLM Rijk and SURF stipulates that Microsoft may in principle only process the personal data that it obtains from, via, or through the use of the online services as a processor and **for three authorised purposes, and only when proportional**. These purposes are:

1. to provide and improve the service,
2. to keep the service up-to-date, and
3. secure.

In accordance with the privacy amendment, Microsoft considers itself to be a processor when processing data on the use of Teams, OneDrive, SharePoint and the Azure AD.

Risks and mitigating measures

The table below shows the one high and six low data protection risks for data subjects, with the mitigating measures government organisations, universities and Microsoft can take.

No.	High risk	Measures government organisations and universities	Measures Microsoft
1.	Content Data processed in the EU accessible for Microsoft if not E2EE	Do not exchange sensitive or special categories of data via Teams calls that are not end-to-end encrypted	Commit to a clear deadline when E2EE will be supported for group meetings and chat
		Use Double Key Encryption for documents with sensitive or special categories of data stored in SharePoint/OneDrive. This includes recordings of Teams meetings. Use Customer Key and Customer Lockbox for other stored personal data	
		Enable E2EE for Teams 1-on-1 calls by default, and instruct end-users to also enable E2EE	Comply with the SCC requirement to inform customers when Microsoft can no longer comply with the data protection guarantees in the SCC
		Create a Teams and OneDrive privacy policy for internal users and guest users, set rules for sharing of files and images. Make employees and guest users accept these rules through Terms & Conditions imposed by Azure AD	
No.	Low risks	Measures government organisations and universities	Measures Microsoft
2.	Structural transfer of Telemetry Data to the USA (until December 2022)	Accept the temporary risk of the transfer of these pseudonymised data while Microsoft is developing the EU Data Boundary	Apply EU Data Boundary to all personal data by the end of 2022 the latest (with known exceptions)
	Possible access from the USA to audit logs, Azure AD and Telemetry Data processed and stored in the EU after 2022	Accept the risk of access to names and e-mail addresses in the Azure AD or consider the use of pseudonyms in the Azure AD.	Inform customers about the actual status per service of the EU Data Boundary
		Don’t use SMS for authentication to prevent the transfer of unencrypted mobile phone numbers to third countries. Instead, use the Authenticator app or a hardware token	
		Use pseudonyms when the Azure AD is used for Single Sign On with external suppliers for employees whose work identity must remain confidential	
	Incidental transfers of pseudonymous data	When using OneDrive and SharePoint, establish policies to	

	to the USA for security purposes	prevent file names and file paths from containing personal data	
3.	Ongoing incidental transfer of usernames / e-mail addresses / pathnames on OneDrive to the USA	Consider the use of pseudonymous accounts for employees whose work identity must remain confidential	
		When using OneDrive and SharePoint, establish policies to prevent file names and file paths from containing personal data	
4.	Lack of transparency Telemetry Data	Regularly use the Data Viewer Tool when available, and compare the results with Microsoft's public documentation	Provide a functional Data Viewer Tool for OneDrive telemetry data on Windows and MacOS
		Use Microsoft's DSAR tool for admins to obtain access to diagnostic data, and compare with an occasional network traffic analysis	Verify compliance with purpose limitation by adding specific audit questions about the contents, use purposes and retention periods of *Required Service Data*.
		Inform employees about their access possibilities via the Data Viewer tool, or by filing a DSAR with the admin of the organisation	Provide more information on the *Required Service Data*, including Office for the Web
5.	Difficulty to exercise data subject access rights to *Required Service Data*	Use Microsoft's DSAR tool to obtain access to diagnostic data, and compare with an occasional network traffic analysis	Improve the DSAR tool for Diagnostic Data
		Support a specific audit by SLM Rijk on Microsoft's collection and use of the *Required Service Data*	Provide a clear and understandable explanation about the contents of the *Required Service Data*
			Let auditors independently verify the explanation why the DSAR tool provides very limited access to *Required Service Data*: data no longer stored, or no personal data collected
6.	Lack of control: personal data shared with Microsoft and third parties as controllers	Disable Controller Connected Experiences	End of Q2 2022: all traffic to Bing removed from SharePoint Online
		Disable access to third party apps in the tab in Teams	Do not send traffic to Cloudflare on Microsoft support pages that are

			accessed from links in Teams settings on the different platforms
		Instruct end users not to use Bing image searches in SharePoint Online (until functionality is removed)	
7.	Employee monitoring system: chilling effect	Turn off functionality in Teams Analytics & reports, use pseudonymisation: do not enable Viva Insights	Comply with art. 25 GDPR privacy by default: disable Teams Analytics & reports by default
		Conduct DPIA prior to use of the analytics tools such as Viva and Teams Analytics & reports, certainly when used in combination with other Microsoft Windows & Office Analytical services	
		Create a policy to prevent use of Teams Analytics & reports as an employee monitoring tool	When an admin opts-in to pseudonymise the data, inform about the consequences for the raw data held by Microsoft

Conclusions
Since June 2019, as a result of the negotiations with SLM Rijk and SURF, Microsoft has implemented many legal, technical and organisational measures to mitigate the risks for data subjects when processing personal data by using Teams, OneDrive, SharePoint and the Azure AD. In reply to the initial findings of this DPIA, Microsoft improved some shortcomings, and provided assurances about its data processing.

However, in view of the Schrems-II ruling and the technical findings described in this report, Microsoft has to make more adjustments and improvements to mitigate the remaining high risk and the six identified low risks. Microsoft should commit to a clear deadline for the application of E2EE to all Teams exchanges., Additionally, Microsoft should become more transparent about the contents of *Required Service Data*, and provide its customers with independent verification of its compliance with the agreed purpose limitation and retention periods for these specific Telemetry Data. Microsoft should enable administrators to opt-in to any new analytics services, based on clear information about the data processing impact.

If government organisations and universities implement all recommended measures, there are no known high risks for the data processing.

Caveat. It is uncertain how the transfer risks will be assessed by the national data protection authorities, in their joint investigation into the use of cloud services by public sector organisations. The results are expected by the end of 2022. For this DPIA the transfer risks have been rigorously assessed, including a separate DTIA. If necessary, this DPIA and DTIA will be updated in 2023.

Introduction

The Microsoft Office 365 Enterprise license includes the use of three different versions of the software. Office can be installed on the computers and laptops of employees (Office 365 ProPlus), installed on smartphones and tablets (mobile Office apps for iOS and Android) and as online applications running in a browser (Office for the Web, also known as Office for the Web).

This report, commissioned by the Strategic Vendor Management office for Microsoft, Google and AWS (SLM Rijk[1]) housed at the Ministry of Justice and Security, is a repeated data protection impact assessment (DPIA) about Office for the Web and the mobile Office apps. The first DPIA was published on 23 July 2019.[2] A second DPIA was published on 30 June 2020.[3] This DPIA was also performed on behalf of SURF, the central IT procurement organisation for Dutch universities.

DPIA

Under the terms of the General Data Protection Regulation (GDPR), an organisation may be obliged to carry out a data protection impact assessment (DPIA) under certain circumstances, for instance where it involves large-scale processing of personal data. The assessment is intended to shed light on, among other things, the specific processing activities, the inherent risk to data subjects, and the safeguards applied to mitigate these risks. The purpose of a DPIA is to ensure that any risks attached to the process in question are mapped and assessed, and that adequate safeguards have been implemented to mitigate those risks.

A DPIA used to be called PIA, *privacy impact assessment*. According to the GDPR, a DPIA assesses the risks for the rights and freedoms of individuals. Data subjects have a fundamental right to protection of their personal data and some other fundamental freedoms that can be affected by the processing of personal data, such as for example freedom of expression.

The right to data protection is therefore broader than the right to privacy. Consideration 4 of the GDPR explains: "*This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity*".

This DPIA follows the structure of the DPIA Model mandatory for all Dutch government organisations.[4]

---

[1] SLM is the abbreviation of the Dutch words Strategisch Leveranciersmanagement Microsoft.

[2] DPIA Microsoft Office 365 Online and Mobile SLM Rijk 23 July 2019, URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/DPIA+Microsoft+Office+365+Online+and+Mobile+SLM+Rijk+23+july.pdf

[3] DPIA Office 365 for the Web and mobile Office apps 30 June 2020, URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps/DPIA+Office+for+the+Web+and+mobile+Office+apps+30+June+2020.pdf

[4] *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017). For an explanation and examples (in Dutch) see:

Because the data processing takes place on a large scale, and the data processing involves data about the communication (be it content or metadata), and involves data that can be used to track the activities of employees, it is mandatory for the Dutch government organisations and universities in the Netherlands to conduct a DPIA based on the criteria published by the Dutch data protection authority.[5]

Umbrella DPIA versus individual DPIAs
Since individual government organisations and universities buy the licenses and determine the settings and scope of the processing by Microsoft, this DPIA cannot address all possible risks. This general DPIA can help the different public sector organisations with the DPIAs they must conduct, but this document does not replace the specific risk assessments they must make. Only the organisations themselves can assess the specific data protection risks, based on their specific deployment, the level of confidentiality of their work and the types of personal data they process.

In GDPR terms SLM Rijk and SURF **are not the data controllers** for the processing of Diagnostic Data via the use of the Office applications. The data controller is the individual government organisation or university that offers the use of the Office software to its employees, guest users and students. However, as central negotiators with Microsoft, they have a moral responsibility to assess the data protection risks for the employees and negotiate for a framework contract that complies with the GDPR. Therefore, SLM Rijk and SURF commission umbrella DPIAs to assist the organisations to select a privacy-compliant deployment, and conduct their own DPIAs where necessary. Only the organisations themselves can assess the specific data protection risks, related to the technical privacy settings, nature and volume of the personal data they process and vulnerability of the data subjects.

This umbrella DPIA is meant to help the different organisations with the DPIA they must conduct, but this document cannot replace the specific risk assessments the different government organisations must make.

Other Microsoft DPIAs SLM Rijk
SLM Rijk has previously assessed the risks for many other Microsoft products and services, such as Windows, Office on multiple platforms, Dynamics, Double Key Encryption and Azure. Microsoft has been working constructively with SLM Rijk during the review of the risks of the use of these products. SLM Rijk is also responsible for the procurement of Amazon Web Services and Google Cloud services, including Google Workspace.

https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia.

[5] Source: Dutch DPA, (information available in Dutch only), Wat zijn de criteria van de AP voor een verplichte DPIA? URL: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667. Similar criteria (data processed on a large scale, systematic monitoring and data concerning vulnerable data subjects and observation of communication behaviour) are included in the guidelines on Data Protection Impact Assessment (DPIA), WP249 rev.01, from the data protection authorities in the EU, URL: http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236.

In November 2018 SLM Rijk published a first DPIA on the data protection risks of the autumn 2018 version of Office 365 ProPlus, version 1708.[6] The report was published on the central Dutch government website with an update on the negotiations between the Dutch central government and Microsoft about the GDPR compliance.[7] In May and June 2020 a (repeat) DPIA was conducted on Office 365 for the Web and mobile Office apps. The DPIA concluded there were 6 high data protection risks for end-users of the software related to the processing of data about their use of the software and services.[8]

Simultaneously with the DPIAs on Office 365, SLM Rijk commissioned a renewed DPIA on Windows 10 Enterprise. SLM Rijk also commissioned DPIAs on the data processing risks of using Microsoft's Azure cloud services, Double Key Encryption and Microsoft Dynamics, and on Google Workspace.[9]

The DPIA reports have been written by the Dutch privacy consultancy firm Privacy Company.[10]

Improvement measures taken by Microsoft

Between **April and June 2020**, SLM Microsoft Rijk and Microsoft agreed on measures to mitigate the six high data protection risks for Office for the Web and the mobile Office apps. As agreed, and verified by Privacy Company, since 1 August 2020, Microsoft had implemented 4 mitigating measures. These were:

1. Provide further information on the third parties identified in the DPIA report and classification of these parties either as a sub-processor (if Microsoft is a processor) or a Controller Connected Experience, a Non-Microsoft Product or an Add-In (if Microsoft is the controller).
2. Roll out controls by which the system administrator can limit or turn off, at the customer's choice, the use of optional/Controller Connected Experiences for the Excel, OneDrive, Outlook, PowerPoint, Teams and Word mobile applications.
3. Roll out controls to limit the collection by Microsoft of Diagnostic Data from the Excel, OneDrive, Outlook, PowerPoint, Teams and Word mobile applications (telemetry limitation choice for admins), plus ensure that all Diagnostic Data collected from Office for the Web will be limited to (the minimum level of) *Required Service Data*.
4. Prevent the presence of certain content (file-, pad-, usernames) in Telemetry Data when using parts of Office for the Web.

In a second check performed in **February 2021**, Privacy Company verified Microsoft's compliance with the remaining improvement measures.

---

[6].URL: https://www.rijksoverheid.nl/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office.

[7] URL: https://www.rijksoverheid.nl/documenten/publicaties/2018/11/12/strategisch-leveranciersmanagement-microsoft-rijk-slm-microsoft

[8] Data protection impact assessment Office 365 for the Web and mobile Office apps, 30 June 2020, URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps/DPIA+Office+for+the+Web+and+mobile+Office+apps+30+June+2020.pdf

[9] URL: https://www.rijksoverheid.nl/documenten/publicaties/2021/02/12/google-workspace-dpia-for-dutch-dpa

[10] URL: https://www.privacycompany.eu/

1. Microsoft has legally guaranteed (in its OST and DPA) that it only acts as data processor of all personal data that Microsoft and its sub-processors process through the Office mobile apps and through Office for the Web. This except for processing through the Controller Connected Experiences and processing through the Apple, Google and Samsung mobile platforms.
2. Microsoft promised to no longer send personal data to third parties if a system administrator has disabled the Controller Connected Experiences. However, the tests showed that Microsoft still sends traffic to Giphy from Outlook Online, and to itself as data controller (to Bing).
3. Microsoft improved transparency about the Diagnostic Data. Since March 2021, Microsoft publishes a more complete overview of the Diagnostic Data collection, including Office for the Web apps.[11] Microsoft also publishes privacy controls for all apps for Windows, MacOS, iOS, and Android.[12] The pages with information about the Diagnostic Data contain a list of the data items and a brief explanation for each item of what it means or represents. The documentation covers the tested apps, as well as other apps. However, the documentation was still far from complete, compared to the events found in the captured network traffic. About 70 to 80% of events was not documented. In reply to this technical verification report, Microsoft explained: "*It appears that several of the events identified relate to and are sent by Office Essential Services. Those events are documented publicly at Essential services for Office - Deploy Office | Microsoft Docs. The remainder are a combination of Required Service Data and Optional Diagnostic Data events.*"[13]
4. Microsoft provides many personal Diagnostic Data to system administrators via its (online) Data Subject Request tool, but does not explain why it does not provide access to any Telemetry Data (for which it is a data processor).
5. Microsoft promised to make the Data Viewer Tool available for more Office apps. Since February 2021, Microsoft provides a Data Viewer Tool for OneDrive, Outlook and Teams on Android and iOS. However, the tool only appeared to function in Teams on iOS and in OneDrive on Android, but did not actually show any Telemetry Data in the tool on Windows 10.

After having been provided with this initial DPIA in **May 2021**, next to the announcement of EU Data Boundaries, Microsoft mitigated several initial high risks and provided explanations to eliminate other concerns.

- In September 2021 Microsoft released new versions of its Data Viewer Tool that enable end-users to inspect the Telemetry Data from Teams and OneDrive on Android, iOS, Windows and MacOS. There is and will be no DDV tool for SharePoint. Privacy Company confirmed the availability and technical functioning of the Windows and MacOS Data Viewer tools for Teams (but not yet for OneDrive) in January 2022 (See Table 2 below).
- Microsoft (accidentally) transferred personal data from Teams on Windows to third parties when an end user visited information about non-Microsoft apps in the apps tab in Teams, and when an end user accessed the privacy settings in Teams on an iPhone. These issues have been mitigated in newer versions

[11] https://docs.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data#office-setup-and-inventory-subtype.

[12] Microsoft, Privacy controls available for Office products, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/products-versions-privacy-controls.

[13] Reply Microsoft 8 June 2021 to questions from the Ministry of Justice and Security following the outcomes of the second technical verification report of 8 April 2021 of Microsoft's compliance with the improvement plan for Office for the Web and the mobile Office apps.

of the app, released since June 2021. Microsoft has explained how administrators can prohibit end users from viewing third party apps in the tab in Teams.

- In reply to a concern about the privacy conditions that would apply to external guest users in Teams, Microsoft provided a guarantee that it protects the privacy of all participants of a Teams conversation initiated by an Enterprise or Education customer by the same privacy guarantees negotiated by SLM Rijk for Dutch government organisations. This protection also covers guest users that participate with their own (consumer) Teams apps. The name or identifier of the government organisation is not collected in the telemetry data from the guest users' application: only the occurrence of the use of Teams for a certain period.
- In reply to a separate concern about unauthorised disclosure of the existence of specific employee accounts through Teams, Microsoft explained that the risks of unauthorised access to the names and e-mail addresses of end users outside a customer's own tenant are low. Microsoft does not provide access to a directory of users of another tenant. Attackers may try to guess names in an automated way, and collect a list of valid addresses from the absence of error reports or login failures. Microsoft has technical protections in place against such brute force attacks. Nonetheless it is possible for attackers to perform specific queries in Teams for specific employees, such as VIPs. This risk is usually not very different from trying to guess an e-mail address for a specific employee, or social engineering to obtain a direct phone number through the reception.

In **February 2022**, Microsoft was provided with this updated DPIA report. Microsoft confirmed the findings, and suggested some factual corrections. For example: the EU Data Boundary will be applied by default to all EU Enterprise and Education customers, and does not require an active opt-in from the admins. Microsoft referred to a public statement that it does not provide, and has *never provided, EU public sector customer's personal data to any government*, even though Microsoft is prohibited from disclosing if it has received orders under secrecy obligation.[14] Microsoft also confirmed *that Teams engineering is working toward supporting E2EE in group VoIP meetings and chat*. With regard to the transfer of Telemetry Data, Microsoft has confirmed these will be exclusively processed in the EU. "*Outside of potential transfers for security purposes, there will not be a physical transfer of EUPI. Instead, any transfer would be limited to remote access that does not permit the data to be retained outside of the boundary.*"[15] Microsoft has informed SLM Rijk it is still investigating if a US fiscal obligation introduced in 2020 applies to Microsoft. This obliges communication providers to retain IP addresses from end users for 3 to 6 years if they want to deduct Foreign-Derived Income. If this applies to Microsoft, this DPIA will be updated.

Scope of this DPIA

This report charts the risks of personal data processing via three commonly used online applications: Teams, OneDrive, and Sharepoint Online in combination with the cloud identity service (Azure Active Directory) on all available platforms. That is: as installed desktop apps on MacOS and Windows, accessed via the browser and as installed mobile apps on iOS and Android. This report also assesses the legal (not technical) risks of unlawful US government access to Content Data stored or

[14] Microsoft, Compliance with EU transfer requirements for personal data in the Microsoft cloud, November 2021, URL: https://go.microsoft.com/fwlink/p/?LinkID=2184913.

[15] Microsoft reply to the Updated DPIA report, 14 February 2022.

processed on Microsofts cloud servers, i.e., the documents, files, emails and conversations in Teams.

Outside the scope of this report

This DPIA does not assess the risks of the data subjects that may result from the use of Windows 10 and other applications in Microsoft Office 365 ProPlus, or other cloudservices of Microsoft that are included in the Office 365 license, such as Skype for Business, Planner, Power BI, EOP/ATP and Intune. Nor in scope are additional services from Microsoft based on Diagnostic Data such as Delve, WorkPlace Analytics and MyAnalytics. However, the new Teams Analytics & reports functionality is in scope, as well as the Diagnostic Data that can be accessed through the Teams Admin Center and the Microsoft 365 Admin Center.

Methodology

Privacy Company applied different investigation methods:

1. the interception and decoding of data traffic from the desktop devices, the Chrome browser and the iOS and Android smartphones,
2. (failed attempt to) inspect the data via the Diagnostic Data Viewer tool,
3. accessing the audit logs,
4. accessing the available Diagnostic Data in Teams Analytics & Reports, and the Teams Admin center,
5. accessing user data in the Microsoft 365 Admin Center,
6. using Microsofts Data Subject Request tool for admins.

Privacy Company performed the analysis on the following devices and platforms.

Table 1: tested applications per device and platform (May 2021)

	Android, Nokia 3, with Android operating system version 9, security patch level 5	iOS, iPhone 7 running iOS version 12.3.1	MacOS, a MacBook with macOS Catalina 11.4	Windows 10, version 21H1	Browser (Chrome), version 90.0.4430.93 (Official Build) (64-bit) on a Macbook pro, with OS version macOS Catalina 11.4
Teams	2020.41.01.2	2020.44.01.7	1.4.00.8872	1.3.00.21759	No version history, tested on 3 May 2021[16]
OneDrive	6.21.1	11.15.8	21.073.0411.0002	6.21.1	No version history, tested on 3 May 2021
SharePoint	4.32.0	4.32.0	Not available	Not available	No version history, tested on 3 May 2021

Specific test scenarios were executed between 30 April and 3 May 2021 in the tested applications (Teams, OneDrive, Sharepoint) on the different devices and in the browser. The scenarios have been developed to reproduce everyday actions of end users.

[16] Microsoft does not display update information or version history for the online versions available through browsers (Office for the Web).

Microsoft appears to make a Data Viewer tool available for the Teams and OneDrive apps on iOS and Android, but the tool only functions well for Teams on Android. No Data Viewer tool is made available for Teams and OneDrive on Windows and MacOS.

During the initial testing, a Data Viewer tool was available for the diagnostic data from the Teams and OneDrive apps on iOS and Android, but it only technically functioned on Teams on Android. No Data Viewer tool was available for Teams and OneDrive on Windows and MacOS. Privacy Company retested the availability and technical functioning of the DDV in September 2021, and in January 2022.

Table 2: tested availability of DDV in January 2022

Operating System	**Teams version no.**	**Available and functioning?**	**OneDrive version no.**	**Available and functioning?**
Android	2020.41.01.2	Yes	6.21.1	Yes
iOS	2020.44.01.7	Yes	11.15.8	Yes
Windows 10	1.4.00.32771 (64-bit)	Yes	6.21.1	Not available
MacOS	1.4.00.34557	Yes	21.073.0411.0002	Not available

The telemetry traffic from the desktops, apps and via the browser is encoded in an undocumented format. As a result, it is not easy to analyse the content of the intercepted telemetry events without a Data Viewer tool. The structure of the events is not entirely clear. Pieces of text are easy to recognise, but some parts of an event are not saved as readable text and are therefore not easy to understand.
Privacy Company tested for a limited period. As a result, Privacy Company did not detect all types of telemetry events. The details of the interception method, and intercepted data, are described in Appendix 1 of this report.

Privacy Company ensured that the research is reproducible and repeatable. This was achieved by working with written scenarios in which the number of actions is limited. There was a pause of 30 seconds between each action. Screenshots have been made of all actions. All data have been recorded. The observed network termination points and the captured telemetry events are recorded in Appendix 1 to this report.

Privacy friendly settings in the test environment
The test tenant was configured according to the previous recommendations from SLM Rijk to mitigate data protection risks for end users. The level of telemetry events was set to the lowest level 'Neither'. The Controller Connected Experiences were switched off, and Giphy in Teams was switched off through a group policy. No changes were made to the default settings for the new functionality of Teams Analytics & Reports. However, the effectivity of the pseudonymisation solution was tested, and thus the central admin settings were changed.

Audit logs and data subject access requests
Microsoft processes usage data on its own cloud servers about the use of Teams, OneDrive, SharePoint and the Azure AD. It is not possible to intercept this data flow from an end-user’s device, because the data processing entirely takes place on Microsoft’s cloud servers.

To gain insight in this data processing, all available log files and reports for admins were accessed. This includes a query in the audit log files with detailed information about the activities performed by the test accounts, as well as the usage data available in the Microsoft 365 Admin Center. Additionally, an (automated) data subject access

request was filed for one of the two test accounts. For this purpose, the dedicated Data Subject Request tool Microsoft offers to administrators was used.

Outline

This assessment follows the structure of the *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017).[17] This model uses a structure of four main sections, which are reflected here as "parts".

1. Description of the factual data processing
2. Assessment of the lawfulness of the data processing
3. Assessment of the risks for data subjects
4. Description of mitigating measures

Part A explains the data processing resulting from the use of the four tested applications on the different platforms in detail. This starts with a description of the technical way the data are collected, and describes the categories of personal data and data subjects that may be affected by the processing, the purposes of the data processing, the different roles of the parties, the different interests related to this processing, the locations where the data are stored and the retention periods. In this section, the measures implemented by Microsoft as a result of the 2019 negotiations with SLM Rijk, as followed-up with improvement plans, have already been processed.

Part B provides an assessment (by Privacy Company, with input from the SLM Rijk and from SURF) of the lawfulness of the data processing. This analysis starts with an analysis of the extent of the applicability of the GDPR and the ePrivacy Directive, in relation to the legal qualification of the role of Microsoft as provider of the software and services. Subsequently, conformity with the key principles of data processing is assessed, including transparency, data minimisation, purpose limitation, and the legal ground for the processing, as well as the necessity and proportionality of the processing. In this section the legitimacy of transfer of personal data to countries outside of the EEA is separately addressed, as well as how the rights of the data subjects are respected.

In Part C the risks for data subjects are assessed, as caused by the processing activities related to the collection of usage data from Office for the Web and the mobile Office apps, but also related to the risks of undue access to the personal data by US government services.

Part D assesses the measures that can be taken by either Microsoft and the individual government organisations and universities to further mitigate the risks as well as their impact.

This DPIA is repeating earlier work and is focussed on verifying the improvement measures agreed by Microsoft. In sections of this report where no changes occur as compared to the previous DPIA report from 30 June 2020, we will refer to this earlier report.

[17] The Model Data Protection Impact Assessment federal Dutch government (PIA). For an explanation and examples (in Dutch) see: https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia

Part A. Description of the data processing

This first part of the DPIA provides a description of the characteristics of the Diagnostic Data collected via Teams, OneDrive, SharePoint Online, in combination with the use of the Azure AD. These applications have been tested on all available platforms (as installed desktop apps on Windows and Mac, via the browser, and as mobile Office apps on Android and iOS. This first section starts with a short description of the processing of different kinds of data (content, Diagnostic Data and functional data).

This section continues with a description of the personal data that may be processed in the Diagnostic Data, the categories of data subjects that may be affected by the processing, the locations where data may be stored, processed and analysed, the purposes of the data processing as provided by Microsoft and the roles of the government organisations and Microsoft as processor and as data controller. This section also provides an overview of the different interests related to this processing, and of the retention periods.

1. The processing of Diagnostic Data

This DPIA provides an overview of the data protection risks caused by the processing of personal data through the use of Teams in combination with OneDrive and Sharepoint Online and the cloud authentication service Azure Active Directory. The data processing is tested on all available platforms (desktop applications, mobile apps and via the browser).

1.1 About Teams, OneDrive, SharePoint Online and the Azure AD

Microsoft Teams is an online communication and collaboration platform that brings together chat, video conferencing, file storage, including shared files, and application integration. It is part of Office 365. Microsoft Teams is used as a successor of Skype for Business.

SharePoint Online and OneDrive for Business offer cloud storage space (hereinafter the official names are abbreviated to SharePoint and OneDrive). These two storage services allow employees to store and share files with each other more easily from the Office software, and from Teams in particular. OneDrive is the basic application to store files. Sharepoint works as an interface on top of OneDrive to allow file storage, and additional options such as the creation of wikis and forms. If a Teams call is recorded, it is automatically stored in the organisation's OneDrive.

If Dutch government or university employees or students want to use Office 365 for work or study purposes, they must have an Office 365 work account and be assigned a license.[18] Office 365 Enterprise and Education accounts and their related licenses are registered in the Azure Active Directory (hereinafter: Azure AD). This is Microsoft's online cloud identity service. Office 365 uses the Azure AD to give people access to

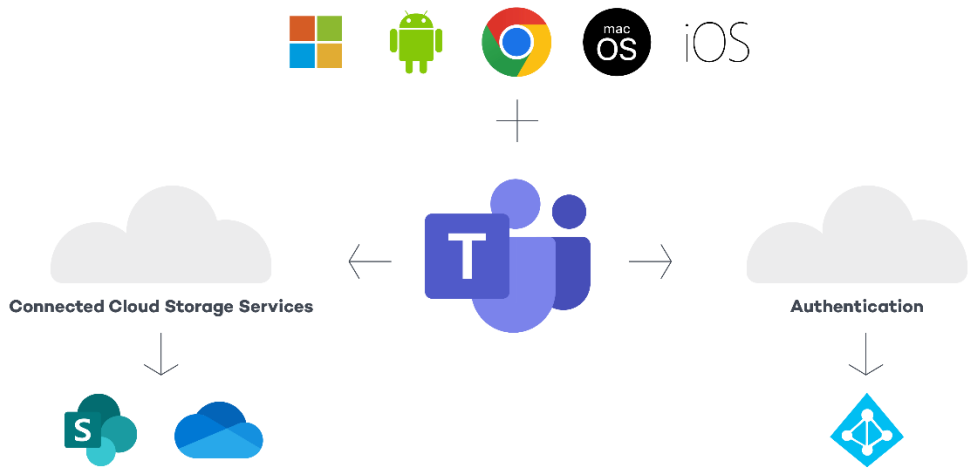
[18] Microsoft explains: "*To use Office 365 ProPlus, a user must have an Office 365 account and have been assigned a license. If the user's license or account is removed, the user's installations of Office 365 ProPlus go into reduced functionality mode. Even though users don't need to be connected to the Internet all the time to use Office 365 ProPlus, users must connect to the Internet at least once every 30 days. This is so that the status of their Office 365 subscriptions can be checked. If users don't connect within 30 days, Office 365 ProPlus goes into reduced functionality mode. After users connect to the Internet and their subscription status is verified, all the features of Office 365 ProPlus are available again.*" URL: https://docs.microsoft.com/en-gb/deployoffice/about-office-365-proplus-in-the-enterprise

Microsoft's cloud services, such as Skype, the Store, SharePoint Online, OneDrive for Business and Exchange Online.

For system administrators, the Azure AD is attractive because the service offers standard support for the cloud protocols OAuth and Saml and can be used for Single Sign On with many other third-party cloud services. The service offers extensive possibilities for adding, updating and deleting users, registering devices and managing the authorisations per user.[19] Through the Azure AD, Microsoft processes the account data of employees and students, including times of sign-in. This logging can be used to derive information about work patterns of end users.

Teams, OneDrive and SharePoint can be used on five different platforms. The software can be installed on the computers and laptops of data subjects, as applications for mobile devices (Android or iOS), and accessed through a browser (for this test Chrome was used).

Figure 1: Scope of this DPIA



Teams and OneDrive include the use of some Connected Experiences such the possibility to insert an image. As part of the negotiated privacy improvement measures with SLM Rijk and SURF, Microsoft offers most of the Connected Experiences as a data processor. That means Microsoft may only process the personal data resulting from the use of these services for the limited set of three purposes as the other Online Services, as determined in the privacy amendment. See the previous DPIA on Microsoft's mobile Office apps and Office for the Web from June 2020 for more details.[20]

[19] See the explanation of Microsoft, Microsoft Cloud Identity for Enterprise Architects, August 7 May 2021, https://docs.microsoft.com/en-us/microsoft-365/solutions/cloud-architecture-models?view=o365-worldwide

[20] DPIA on Microsoft Office 365 for the Web and mobile Office apps, published 30 June 2020, URL: https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps

However, for some of these included cloud services Microsoft continues to act as data controller. In the tested three applications the following five Controller Connected Experiences were available:

1. Giving Feedback to Microsoft
2. Insert Online Pictures (using Bing)
3. Insert an image from Giphy (can only be disabled through Group Policy)
4. Suggest a Feature
5. Contact Support

These are called Controller Connected Experiences. In its public explanation and in the interface for admins, Microsoft confusingly distinguishes between four types of Connected Experiences, which partly overlap each other:

1. services that analyse your content,
2. services that download online content,
3. other services
4. Additional Optional Connected Experiences.[21]

Services that fall into the group Additional Optional Connected Experiences are the Controller Connected Experiences. The Additional Optional Connected Experiences are also included in the other three groups of Connected Experiences that Microsoft publishes, for instance if that service also analyses content. This is the case if a service uses search engine Bing or the social network LinkedIn. However, if an admin disables the Additional Optional Connected Experiences, access to all controller services should be blocked, also from the three other groups. This does not apply to Giphy: admins have to apply a separate group policy in Teams to block the access for employees.

Following the privacy recommendations from SLM Rijk after previous Microsoft Office DPIAs, admins should set the level of telemetry events to the lowest level of 'Neither'. The Controller Connected Experiences must be switched off, and Giphy in Teams should be disabled through a group policy. See Section 3.1 for a description with screenshots of these options. For this DPIA all these recommendations were followed in the test *tenant*.

1.2 Difference between Content, Functional and Diagnostic Data

Inspired by the e-Privacy directive, this report distinguishes three categories of data that Microsoft processes as service provider.

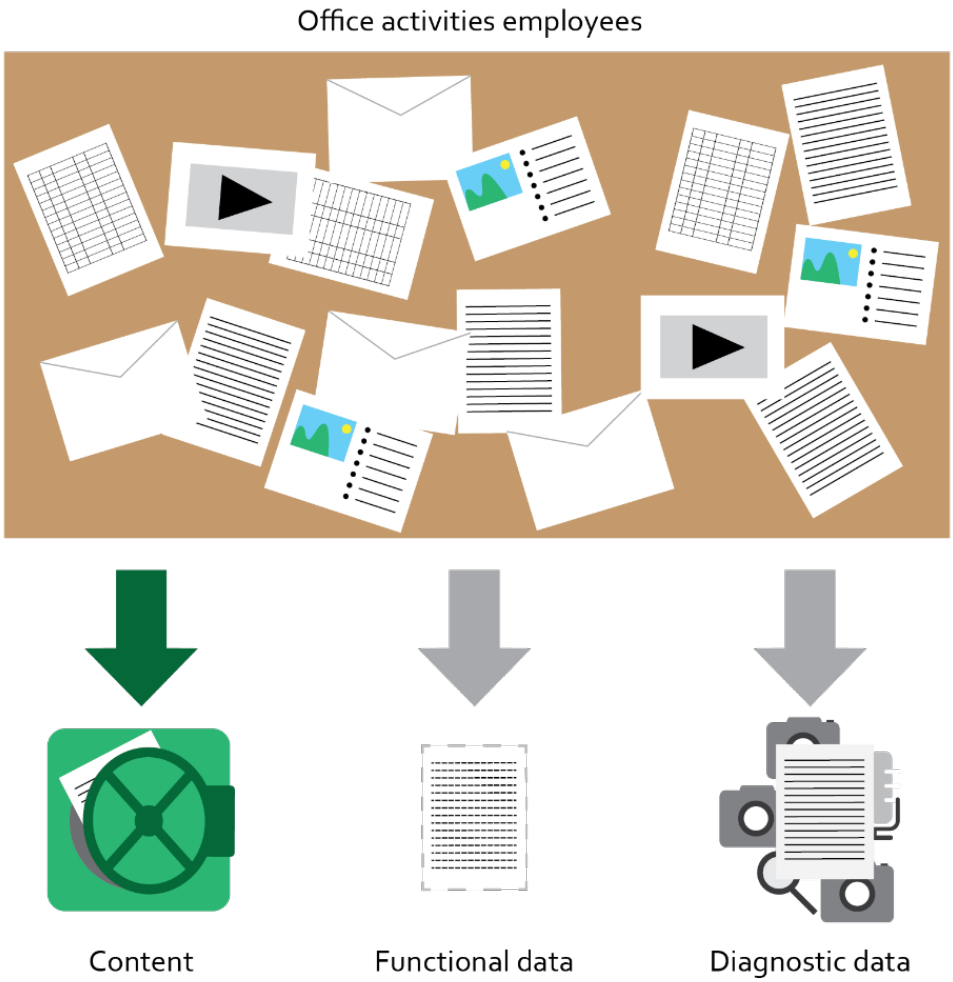
Content of the communication with Microsoft-services. For a part of these Content Data, so called Customer Data, Microsoft offers separate guarantees. This category includes file- and path names on SharePoint and OneDrive.

Diagnostic data, which is all data Microsoft saves in logfiles about the behaviour of individual users and its services, whether these are telemetry files first collected on a computer or smartphone and then sent to Microsoft, or data in system-generated cloud server logs.

[21] Microsoft, Connected experiences in Office, 14 January 2020, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/connected-experiences and Microsoft, Overview of optional connected experiences in Office, 14 January 2020, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/optional-connected-experiences

Functional data, which are only necessary for the transfer of communication. These data are functional, and outside the scope of this DPIA, to the extent they are deleted or anonymised directly after completion of the transfer of communication, in line with the rules in the e-Privacy directive. These rules officially apply to the use of Teams as an electronic communications service since December 2020.[22]

Figure 2: Content data, Functional Data and Diagnostic Data



In this report, all data about the individual use of Teams, OneDrive and SharePoint, as well as all logfiles about signing into the Azure AD are called Diagnostic Data, but only to the extent that they are stored by Microsoft and not merely transported. This includes system-generated event logs and so called 'Telemetry Data' collected from the mobile Office apps that are regularly sent to Microsoft's servers

[22] Since the European Electronic Communications Code (EECC) became applicable law (21 December 2020) , the confidentiality rules in the ePrivacy Directive apply to all over-the top communications services, such as Microsoft with Teams, and other providers of internet-based videoconferencing services. See Section 9 of this report.

The term functional data is used for all data that must be sent from the user's device to communicate with Microsoft's online communication and storage services. Examples of such functional data are the data stream necessary to allow the user to store a text file on Microsoft's cloud storage service OneDrive, or the data stream necessary to authenticate or to verify if the user has a valid license. The main difference between functional data and Diagnostic Data as defined in this report, is that functional data are and should remain transient.[23] As long as Microsoft doesn't store these functional data, or if the data are not personal data during collection (for example data about the temperature of a CPU in a server), they are not Diagnostic Data and therefore out of the scope of this DPIA.

1.3 Different types of Diagnostic Data

Microsoft processes different kinds of Diagnostic Data about the individual use of the three tested applications. These metadata (about the individual use of the services and software installed on phones) are referred to in this report as 'Diagnostic Data'.

> Diagnostic data in this report are both the so-called Telemetry Data, events sent systematically to Microsoft from the mobile Office apps and Office for the Web, and the data that Microsoft generates and stores on its own servers about the individual use of the Office services, the so-called system-generated event logs.

Sometimes the Diagnostic Data also contain Content Data, such as file- and path names when using SharePoint and OneDrive. The Azure AD generates another category of metadata, about the use of the online authentication service Azure Active Directory.

Microsoft systematically collects Telemetry Data about the use of its software via a built-in telemetry client. This is software that records all the actions a user performs and regularly sends these data, in batches, to Microsoft's servers in the United States. The client is built into installed apps on desktops/laptops, on mobile devices and in the browser version of the apps. The Diagnostic Data are sent in an undocumented binary format. Since the spring 2019 version (version 1904) of the Office 365 ProPlus software, Microsoft has made a tool available in some apps, on some platforms, for end users to view the data themselves in a readable form. This can be done using the same Data Viewer Tool that Microsoft has been offering since the spring of 2018 to provide insight into the contents of data about the individual use of Windows 10. That means end users and admin must have access to a device with Windows 10 as the operating system to see the Office Telemetry Data.

Since February 2020, Microsoft has made the Data Viewer suitable for telemetry from Word, PowerPoint and Excel, but not for the other apps, and not for any telemetry from the browser (Office for the Web). In Office for the Web, the default level is set

[23] Compare Article 6(1) of the EU ePrivacy Directive (2002/58/EC, as revised in 2009 by the Citizens Rights Directive) and explanation in recital 22: "*The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit* ***any automatic, intermediate and transient storage*** *of this information in so far as this takes place* ***for the sole purpose of carrying out the transmission*** *in the electronic communications network and* ***provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes****, and that during the period of storage the confidentiality remains guaranteed.*"

to the (lowest) level of *required data*. Microsoft has ensured SLM Rijk it has limited the amount of telemetry events to a minimum, and has contractually agreed to never include any Content Data in these events.

In addition, Microsoft collects detailed personal information about the use of its Office applications in log files of its cloud servers. Microsoft records those usage data in so-called system-generated event logs. These logs contain data about the use of Teams, OneDrive, SharePoint and the Azure Active Directory. Microsoft makes some of these Diagnostic Data available through audit logs and reports for admins.

2. Personal data and data subjects

The Dutch government DPIA model requires that this section provides a list of the kinds of personal data that will be processed via the Diagnostic Data, and per category of data subjects, what kind of personal data will be processed by the product or service for which the DPIA is conducted. Since this is an umbrella DPIA, this report can only provide an indication of the categories of personal data and different kinds of data subjects that may be involved in the data processing by specific organisations.

The section about personal data provides legal, technical and organisational arguments why the Diagnostic Data processed by Microsoft about the individual use of the applications are personal data.

This section 2 provides a technical analysis of the Telemetry Data from the tested applications on all platforms as documented by Microsoft and the comparison of these data with the network traffic that was intercepted with the proxy. This section also discusses the results of the analysis of the Diagnostic Data made available to admins in audit logs, through a content search in the Security & Compliance Centre, and through the Admin 365 center.

2.1 Definitions of different types of personal data

The definition of personal data is defined as follows in Article 4(1) of the GDPR:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

Microsoft collects personal data directly from customers and indirectly, through the use of its services.

In the privacy amendment that SLM Rijk concluded with Microsoft for the central Dutch government, the different types of personal data that Microsoft processes from, about and through the use of its online services are all defined as personal data. This privacy amendment also includes a definition of anonymisation, with reference to the guidelines of the Article 29 Working Party (the European data protection authorities now united in the European Data Protection Board).

In January 2020, Microsoft changed its Online Service Terms (OST) for Enterprise customers worldwide, and included all relevant privacy statements in a separate Data Protection Addendum for Microsoft Online Services (hereinafter: DPA).[24]

In its DPA of September 2021, under the heading 'Processing of Personal Data; GDPR' Microsoft explains: *"All Personal Data processed by Microsoft in connection with providing the Products and Services is obtained as part of either (a)* ***Customer Data****, (b) Professional Services Data, or (c)* ***data generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer's use of service-based capabilities or obtained by Microsoft from locally installed software****. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Online Service is also Customer Data. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Professional Services is also Professional Services Data.* ***Pseudonymized identifiers may be included in data processed by Microsoft in connection with providing the Products and are also Personal Data.*** *Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data."*[25]

For Enterprise customers that cannot benefit from the Dutch government's privacy amendment, it is a major improvement that Microsoft describes the two types of Diagnostic Data (*Customer's use of service-based capabilities* or *obtained by Microsoft from locally installed software*) it collects, and that Microsoft explicitly acknowledges that pseudonymised or de-identified data are personal data, including diagnostic data.

2.2 Telemetry data mobile Teams, OneDrive and SharePoint apps

As explained in Section 1.3, Microsoft collects two types of diagnostic (meta)data about the individual use of it services: Telemetry Data and service generated data in server log files. This section describes the Telemetry Data collected from end-user devices, while section 2.3 describes the other Diagnostic Data, generated on Microsoft's cloud computers.

Microsoft has developed the Office desktop and mobile apps to include a telemetry client. Since the spring of 2020, Microsoft has also programmed a client to collect Telemetry Data on the device when using the applications through a browser (Office for the Web). The clients send the Telemetry Data *in batches* to Microsoft on a regular basis.

Since 2019, as a result of the improvement plan agreed with SLM Rijk, Microsoft has made three major global improvements to mitigate data protection risks resulting from the processing of Telemetry Data. Microsoft:

1 offers choices for admins to minimise the amount of collected Telemetry Data[26];

[24] Microsoft Online Services Data Protection Addendum. The most recent public version from the DPA dates from 15 September 2021, URL: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

[25] Ibid.

[26] Microsoft, Microsoft, Overview of privacy controls for Microsoft 365 Apps for enterprise, 30 September 2021, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/overview-privacy-controls

2 publishes detailed information about the different telemetry events in the different applications on different platforms, for the different telemetry 'levels'[27], and

3 makes a Data Viewer Tool available for end users to inspect the Telemetry Data for an increasing amount of Core Office applications and platforms (though not for the browser-based telemetry).[28].

None of the three described improvements apply to the Telemetry Data generated by Office for the Web (when Office applications are accessed through a browser). There are no data minimisation choices for these Telemetry Data, there is no public documentation and Microsoft will not develop an end user inspection tool for these Telemetry Data.

Microsoft explains: "*With regard to Office 365 Experiences that are available solely while online (such as the case for Office for the Web and Microsoft Teams and OneDrive for Business, and most Microsoft mobile platform applications) the online service Diagnostic Data is required Diagnostic Data and the control setting of "Neither" for Diagnostic Data has no effect. There may also be no additional "optional" Diagnostic Data and thus no effect for that control. In most cases those Diagnostic Data controls are specific only to applications that have fully functional offline use-cases (e.g., Microsoft Word running on Windows 10 or MacOS).*"[29]

In 2020 and 2021, Microsoft steadily increased transparency for Teams and OneDrive. Since September 2020, as agreed in the improvement plan with SLM Rijk and SURF, Microsoft publishes specific information about the contents of the Telemetry Data it collects about Teams when used on a desktop[30] and since May 2021, also for the data collection in the mobile Teams apps.[31] No such information is or will be made available for SharePoint, as Microsoft does not consider SharePoint to be a Core Service in Office.

In the second half of 2021, Microsoft expanded the availability of the Diagnostic Data Viewer (DDV) to the iOS and Android apps for Teams and OneDrive. The functionality of these tools was confirmed in the most recent app versions in January 2022. The DDV is not yet available in the desktop versions of OneDrive (Windows and MacOS).

In May 2021 the DDV was tested for Teams on Android. The visibility was limited to two types of events. In the limited re-tests performed in January 2022, the Data Viewer Tool similarly showed very few events. These events were compared to the telemetry events that could be recognised in the captured network traffic. This traffic analysis shows that **Microsoft only documents and shows 10 percent of the**

---

[27] Microsoft, Required diagnostic data for Office, 20 January 2022, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data

[28] Microsoft, Using the Diagnostic Data Viewer with Office, undated, URL: https://support.microsoft.com/en-us/office/using-the-diagnostic-data-viewer-with-office-cf761ce9-d805-4c60-a339-4e07f3182855

29 E-mail Microsoft to Privacy Company, 6 March 2020.

[30] Microsoft, Required desktop Diagnostic Data for Microsoft Teams, 27 August 2021, URL: https://docs.microsoft.com/en-us/microsoftteams/policy-control-diagnostic-data-desktop

[31] Microsoft, Required mobile Diagnostic Data for Microsoft Teams, 19 May 2021, URL: https://docs.microsoft.com/en-us/microsoftteams/policy-control-diagnostic-data-mobile

collected Telemetry Data about the individual use of Teams, SharePoint and OneDrive. As shown in Appendix 1, approximately 90% of the detected telemetry events in the captured network traffic are undocumented and invisible in the Diagnostic Data Viewer. According to Microsoft all events observed in the captured network traffic, that were not documented, belonged to the category of *Required Service Data*.[32] It is not clear when Microsoft classifies an event as *Required Service Data*, but it appears to include three kinds of telemetry events. Events originating from Office for the Web, events due to the use of the different kinds of processor and controller Connected Experiences and events due to what Microsoft calls 'Essential Services' of Office, such as the licensing service.[33] In reply to this DPIA Microsoft explained to SLM Rijk that it will not publicly document, nor show in the Data Viewer, telemetry events belonging to this category of *Required Service Data*. However, Microsoft publicly promises to provide access to these telemetry data when an admin uses Microsoft's tools to respond to Data Subject Access Requests (DSAR). The output of these DSAR tools is discussed in Section 2.5 below.

Microsoft provides the following arguments for this lack of transparency: there are too many data, that change too frequently, thus making documentation too costly, and some data are company confidential.

"*As discussed, and per our public documentation, Microsoft processes the data necessary to provide a service, and keep it secure, up to date and performing as expected (referred to as Required Service Data (RSD)). Microsoft provides categorical descriptions and examples about RSD in public facing documentation but does not publish the same event-level documentation as provided for Required Diagnostic data processed from client application software. Services are dynamic/ever-changing and typically involve and require processing more data (as compared to data processing from client application software running on a user device) to provide the applicable service, and keep the service secure, up to date and performing properly, making it commercially unfeasible to maintain such detailed event level information. In addition, service-related event level information regularly includes confidential security or other proprietary information about the operation of our services, where publication of such data could put our services, and thus our customers and Microsoft, at risk. For these reasons, we endeavour to provide descriptions of the nature of data processing with useful examples to help our customers understand the types of data processed and why it is necessary* [underscoring added by Privacy Company]."[34]

Microsoft provides the following principles for the data collection in *Required Service Data*:

- *Data will be collected about the usage, performance, and error encountered by the application.*
- *Metadata about the operating system, device and application will be collected to help classify issues.*
- *No content will be collected in data processed for diagnostics.*

[32] E-mail Microsoft to SLM Rijk, 10 December 2021.

[33] Microsoft, Manage required service data, 30 September 2021, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/required-service-data

[34] E-mail Microsoft to SLM Rijk, 10 December 2021.

- *The information will be associated with a logged in user through the use of a pseudonymous identifier.*

- *Additional non-personal identifiers may be included such as a Session ID or Client ID which do not identify a specific individual user."*[35]

Absent well-functioning Data Viewer functionality, the analysis of the contents of the telemetry events is based on the captured outgoing data traffic to the known telemetry domains. It was technically not possible to fully analyse the data captured from the mobile devices. Because Microsoft has not published documentation with the specifications of the binary format in which it enciphers the data, Privacy Company has made a best effort to distil the contents from the intercepted Telemetry Data in the network traffic.

Microsoft publicly promises that telemetry events may only contain pseudonymised identifiers, never names, e-mail addresses or content from files.

Figure 3: Microsoft promise of pseudonymisation of Diagnostic Data[36]

> **Note:** Diagnostic data may contain "personal data" as defined by Article 4 of the European GDPR, but it does not contain your name, your email address, or any content from your files. All diagnostic data Microsoft collects during the use of Office applications and services is pseudonymized, as defined in ISO/IEC 19944-1:2020, section 8.3.3.

It is plausible that all diagnostic messages, just like the messages Microsoft collects on Windows and Office ProPlus, contain a header, and content. A typical diagnostic message contains a unique number, a few unique identifiers for the end user, their account and/or the license administrator (the tenant) and/or their device. These are typical header data. In addition, the messages contain content about the individual use of the various applications.

The research from May 2021 shows that all readable captured events from Teams, OneDrive and SharePoint at least contain the device identifier DeviceInfo.Id. The telemetry also contains a field 'UserInfo.Id' that contains a UUID (non-human readable) identifier for the user account. All events also contain the event EventInfo.Time. This telemetry message contains the unique identifier of the device and the exact time, up to seven decimal places, that the event took place. This allows Microsoft to link different activities of a single user over time. All events contain a Correlation Vector. Microsoft explains on GitHub that this unique ID is included for 5 purposes, including "*to track causality (partial order) of the flow, Provide a simple sort independent of system clock time and Provide the sort/causality tracking capabilities for any arbitrary subset of events in the trace*".[37]

Appendix 1 contains tables with the observed domains in network traffic and types of telemetry events per application per platform. In this appendix the technical research method is also further explained, with examples of the content of intercepted

[35] Idem.

[36] Microsoft, Diagnostic data in Office, undated, last visited 30 January 2022, URL: https://support.microsoft.com/en-us/office/diagnostic-data-in-office-f409137d-15d3-4803-a8ae-d26fcbfc91dd

[37] Microsoft on GitHub, CorrelationVector 2.1, URL: https://github.com/microsoft/CorrelationVector/blob/master/cV%20-%202.1.md

telemetry events. In the limited re-tests performed in September 2021 and January 2022, no previously unknown diagnostic events were observed.

The fact that the telemetry events always contain a device identifier and a (scrambled) user identifier make it possible for Microsoft to identify the individual data subject that has caused the event. Thanks to the recorded type of activity, timestamp and correlation vector ID, Microsoft is able to link multiple events to a single data subject. Therefore, all events are personal data.

Microsoft offers system administrators of the Enterprise and Edu versions of the Office 365 the option of minimising the level of telemetry in the desktop and mobile apps (as explained above, not for Office for the Web). For this DPIA the telemetry level was set to the lowest level: 'Neither'. However, the technical analysis shows that there is **an exception to the rule that Microsoft never includes usernames at this (lowest) level of telemetry. The use of OneDrive may result in the processing of these directly identifiable data in the OneDrive URLs when a document is accessed or shared.**

2.2.1 Reply Microsoft to the observation of readable usernames in OneDrive events

In reply to this finding (in fact, in reply to an earlier finding in February 2021 of the same occurrence of readable usernames in some Telemetry Data), Microsoft explained that this collection of directly identifiable personal data is necessary, that the data are collected through a separate telemetry pipeline, are only used for limited bug fixing purposes in a role as processor, are retained less than 30 days, and are protected with more stringent access controls.

Microsoft writes:
"*OneDrive have Required Service Data flows that involve sending resource strings that may contain End User Identifiable Information (EUII) from client software to Microsoft for purposes of ensuring high quality of service in areas of product reliability, correctness, and performance. These flows are categorized as and limited to Quality of Service (QoS) events and are required for the proper functioning of OneDrive. All data within these RSD workflows remain inside the trusted (audited) O365 compliance boundary. Access to this data is audited, limited to just-in-time security group, and limited to engineers that have an approved business justification. All data from these workflows has data retention of less than 30 days."*[38]

Microsoft states this is a unique exception to the rule quoted above [underscored] that the *Required Service Data* should not contain end user identifiable (non-pseudonymised) personal data. "*For clarity, this is a specific exception to the foundational principles as shared earlier and we see this as a unique situation related to limited End User Identifiable Information in RSD Diagnostic Data for the OneDrive for Business client.*"

The reason why this particular data collection is only necessary in OneDrive, is the possibility for multiple users to work on the same file. If such access puts too heavy a burden on the system, this may negatively influence the availability of other files.

Microsoft explains: "*OneDrive uses programmatic analysis to detect and mitigate situations where excessive and/or expensive requests to specific resources or resource areas either exceed quotas or start to impact the reliability of not only access*

[38] E-mail Microsoft to SLM Rijk, 23 December 2021.

to the specific resource but also the broader resource area. This programmatic analysis can result in dynamic implementation of throttling where some or all the requests are rejected for short periods of time. To accomplish this goal of protecting the reliability of the service for these types of scenarios, the attributes in the aforementioned resource string are needed, including one or more of Tenant Name (OII), File Path (EUII), Username, and/or Email Address."[39]

Microsoft does not yet provide a public explanation about this collection, or the purposes on its information page about the *Required Service Data*.[40]

In sum, except for the directly identifiable username in the Telemetry Data related to the use of OneDrive, Privacy Company **did not observe any directly identifying personal data in the intercepted telemetry events. The events did not contain information from the content, about file names or other user supplied data such as device or profile names.**

With the exception noted above, the information the telemetry events contain appears adequate, and not excessive, for the purpose of measuring what functionalities of the applications are used on the different platforms.

2.3 Outgoing traffic to third parties

In June 2020, Microsoft agreed as privacy improvement measure with SLM Rijk and SURF not to allow any traffic to third parties from any Office 365 apps on any platform, if an admin had blocked the Controller Connected Experiences.

Generally, no third-party traffic was observed during the tests in May 2021 from the apps to undocumented third parties. However, there were three exceptions:

1. Traffic to third parties from Teams on Windows.
2. A failure to block Bing as a Controller Connected Experience in Sharepoint Online (accessed through the browser).
3. Traffic to Cloudflare if a user accessed the privacy settings in Teams on iOS, from the domain support.microsoft.com.

2.3.1 Traffic to third parties via Teams on Windows

Traffic was observed from Teams used on Windows to **Teams.Polly.AI**. Polly is a brand name of Current Inc. According to its job openings, Current.Inc. is "*a remotely-based, distributed team located in various parts of the US, Canada, and Pakistan*."[41] Polly offers survey tools, and can be installed as separate app in Teams.

The technical analysis of the intercepted traffic data showed that the traffic to Polly set in motion a chain of events, resulting in the transmission of unique identifiers to

[39] Idem.
[40] Microsoft, Required service data for Office, 30 September 2021, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/required-service-data
[41] Polly, job opening for Customer Success Manager, URL: https://boards.greenhouse.io/polly/jobs/5149821002

several third parties and tracking cookies. This traffic was due to the appearance of a thumbnail of the Polly app in the section for external apps in Teams.

In the initial data stream, an iframe was loaded in the user interface. Microsoft sent the user agent, referrer (generic) and IP address of the end user to Polly. This initial stream did not contain cookies or tracking identifiers.

However, Polly in its turn generated traffic to four external parties.

- Intercom.io en Intercomcnd.com
- Stripe.com
- The traffic to Stripe includes loading of YouTube YSC cookie
- YouTube in turn loads Google DoubleClick IDE tracking cookie

Figure 4: Example of tracking cookie set by Google DoubleClick

```
set-cookie:

IDE=AHWqTUl5WpME3LFICYyWDKoRhq2AjVXzKK-pK2XJ3hxQRHOKTutJRcrkp3Y6SWuw;
expires=Sat, 28-May-2022 11:21:14 GMT; path=/; domain=.doubleclick.net; Secure; HttpOnly;
SameSite=none
```

YouTube set three cookies. The first cookie is assumed to be a tracking cookie, in view of Google's own explanation: *"For example 'YSC' is used by YouTube to remember user input and associate a user's actions."*[42]

Figure 5: Examples of cookies set by Google YouTube

```
set-cookie:
YSC=170cSj1mvek; Domain=.youtube.com; Path=/; Secure; HttpOnly; SameSite=none

set-cookie:
VISITOR_INFO1_LIVE=qo3Sru9lQ3I; Domain=.youtube.com; Expires=Sat, 30-Oct-2021
11:21:12 GMT; Path=/; Secure; HttpOnly; SameSite=none

set-cookie:
CONSENT=PENDING+531; expires=Fri, 01-Jan-2038 00:00:00 GMT; path=/;
domain=.youtube.com
```

The traffic to the Irish company Intercom and the US based company Stripe (with EU HQ in Dublin) did not result in cookies or transmission of unique identifiers. However, the traffic to YouTube and Google resulted in the placement of *tracking cookies* on the end user device. See Appendix 1 for the details of the transferred data.

In reply to this DPIA, Microsoft explained that administrators can disable access to non-Microsoft apps in this Teams store for end users. Privacy Company has verified that this option is effective in preventing traffic to third parties in the Teams store. See Section 3.1.5.

[42] Google, cookies, URL: https://policies.google.com/technologies/cookies?hl=en-US

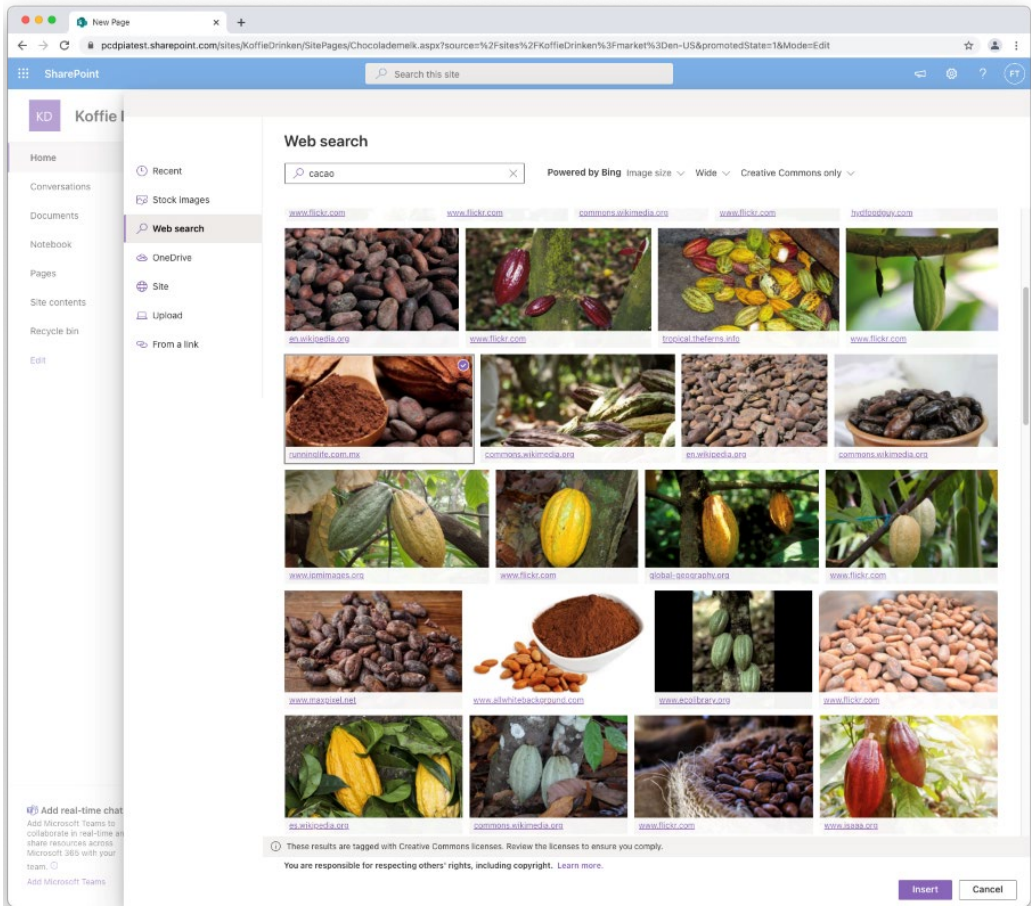
2.3.2 *Traffic to Bing in SharePoint Online (browser)*

When SharePoint was accessed through a browser, it sent user information such as the username, IP address and the name of the organisation to Bing when a user inserted a picture. See Figure 6 below.

In reply Bing sent three cookies with unique identifiers.

Microsoft considers itself an (independent) data controller for all personal data processed by Bing. The functionality of inserting a picture should not be available when the Controller Connected Experiences are switched off by the admins of the government organisations and universities.

Figure 6: Inserting a picture in SharePoint Online



In reply to this finding, Microsoft has committed to remove Bing image searches from SharePoint when a customer has disabled the Controller Connected Experiences before 1 July 2022.

2.3.3 *Traffic to Cloudflare in references to Microsoft support pages*

When an end user wants to view the privacy settings in Teams, selects Settings, clicks on Privacy and then on Diagnostic data, he or she is redirected to a webpage on the

Microsoft Support portal.[43] This page generates traffic to the US content delivery network Cloudflare. Cloudflare is not a subprocessor for Microsoft's Online Services. The screenshots and contents of the GET request to Cloudflare are included in Appendix 1. Though Microsoft committed to remove this traffic, a retest in January 2022 shows that this webpage still contains a reference to a jQuery (JavaScript file) hosted on Cloudflare.

2.4 Diagnostic data from audits logs and admin consoles in Teams, OneDrive and Sharepoint

For this DPIA an analysis was conducted on all available personal data about the two test accounts which Microsoft makes available to administrators of a tenant.

These are:

- The audit logs
- Teams Analytics & Reports and user data in the Teams Admin center
- User data in the Microsoft 365 Admin Center

Microsoft does not provide any specific information about its diagnostic data collection via its cloud storage services. Microsoft describes in its DSAR manual which actions it records in audit logs, and that these logs are important when an access request is submitted for an end-user.

2.4.1 Audit logs

By default, Office 365 doesn't collect audit logs unless the admin enables them in the Office 365 Compliance centre. In the test set-up for this DPIA, there was an error preventing the admin from turning on the audit log. However, in February 2021 Privacy Company performed a check on Microsoft's compliance with the improvement plan for SLM Rijk. During this test it was possible to conduct such a query (on an active Business tenant with more than two active end users).

Through a Search Content query administrators can access these logs. They register access to the data Microsoft defines as Customer Data, both by the users of the software and by Microsoft employees. In February 2021, Privacy Company observed that these logs contained information about the use of Exchange Online, SharePoint Online en OneDrive.[44]

The following fields appeared in each event:

- UserType

[43] https://support.microsoft.com/en-us/office/using-the-diagnostic-data-viewer-with-office-cf761ce9-d805-4c60-a339-4e07f3182855

[44] Microsoft, Office 365 Data Subject Requests for the GDPR, URL: https://docs.microsoft.com/en-gb/microsoft-365/compliance/gdpr-dsr-office365?toc=/microsoft-365/enterprise/toc.json#part-2-responding-to-dsrs-with-respect-to-insights-generated-by-office-365 (URL last visited and recorded on 31 May 2021). Microsoft explains: "*Product and service usage data for some of Microsoft's most often-used services, such as Exchange Online, SharePoint Online, Skype for Business, Yammer and Office 365 Groups can also be retrieved by searching the Office 365 audit log in the Security & Compliance Center. For more information, see Use the Office 365 audit log search tool in DSR investigations in Appendix A.*"

- UserKey
- RecordType
- Id
- UserId
- Version
- OrganisationId
- Workload
- Operation
- CreationTime
- ObjectId

Other events occurred depending on the type of activity, such as the name of the application used (ApplicationID and ApplicationDisplayName), actions such as editing, viewing, uploading, downloading or renaming a file or folder (FileModified, FilePreviewed, FileAccessed, FileUploaded, FileDownloaded, FileRenamed, FolderCreated, FolderModified), logging in, giving or withdrawing sharing permissions, adding to a group, or creating a list. These events contain additional unique identifiers, such as ClientIP and CorrelationID, and content information, such as SiteURL, SourceFileName, WebID, and SourceRelativeUrl.

The log files about the two different test users demonstrate that a directly identifiable person performed an action at a specific time in a tested app, with which browser and from which operating system. This is expected behaviour, as these logs are created for security purposes and necessarily show a trail of all actions with personal data, by identifiable end users. Microsoft also records whether there was a login error, what the cause was, and how the user was authenticated. The users are directly identifiable by the fields with the username and the email address. These access files also contain the used IP addresses.

Because each log line contains the combination of UserId and Organisation ID, each log line is personal data. In addition, these log files contain information about actions on the servers, and Content Data from names of paths and files.

2.4.2 Microsoft 365 admin center

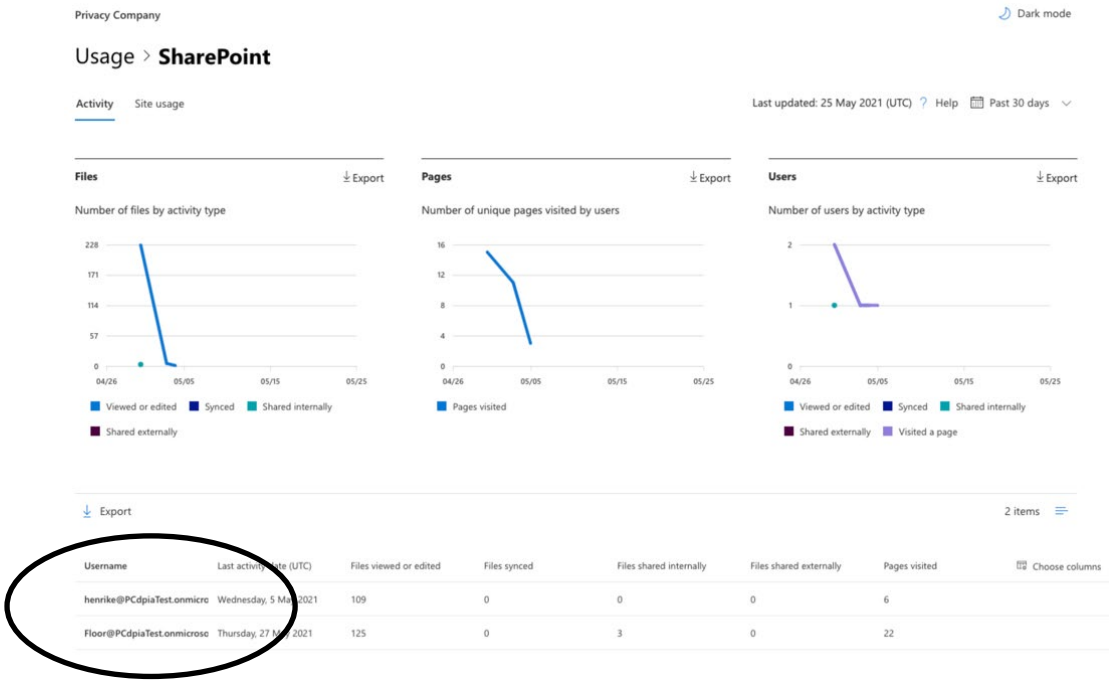
By default, admins have access to Activity Reports in the Microsoft 365 admin center. Through Activity Reports in the Microsoft 365 admin center Microsoft enables administrators to create detailed reports on all kinds of activities per user, such as use of Teams and activity in OneDrive and SharePoint.[45] Microsoft explains: *"Reports*

[45] Microsoft, Activity Reports in the Microsoft 365 Admin Center, 19 May 2021, URL: https://docs.microsoft.com/en-gb/office365/admin/activity-reports/activity-reports?view=o365-worldwide

are available for the last 7 days, 30 days, 90 days, and 180 days. Data won't exist for all reporting periods right away. The reports become available within 48 hours."[46]

If an admin selects an individual application, such as Teams, the names of the end users who have performed the recorded activities are shown in the console. Admins do not have an option to disable the username. See Figure 7 below.

Figure 7: SharePoint usage reports with individual user names



2.5 Results access requests

To gain insight in this data processing, (automated) data subject access requests were filed on 25 May 2021 for the two test accounts by the administrator in the dedicated Data Subject Request tool Microsoft offers to administrators for this purpose.

Microsoft offers several types of tools for admins to respond to data subject requests. For this DPIA, two tools are relevant:

1. Searching the audit log in the compliance center

2. Perform a query for system-generated logs

Through the Content Search in the Security & Compliance Center[47] admins can obtain access to the diagnostic data generated on Microsoft's cloud servers as a result of the individual use of the online services. Microsoft explains it can take up to 30 minutes

[46] Idem.

[47] Microsoft, Search the audit log in the compliance center, 15 January 2022, URL: https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

or up to 24 hours after an event has taken place before the results appear in an audit log search.

In May 2021, the results of these searches consisted of the following fields: ExportItem Id, Item Identity, Document ID, Selected, Duplicate to Item, Original Path, Location, Location Name, Target Path, Document Path, Subject or Title, Sender or Created by, Recipients in To line, Recipients in Cc line, Recipients in Bcc line, To – Expanded, CC – Expanded, BCC – Expanded, DG Expansion Result, Sent, Has Attachments, Importance, Is Read, Modified by, Type, Received or Created, Modified Date, Size (KB), Decode Status, Compliance Tag, Summary, Preservation Original Url.

Through these fields, Microsoft for example registered that investigator Floor Terra (owner of one of the two test accounts used by Privacy Company) created a meeting appointment to discuss a (fictional) meeting about a Corona infection.

Table 3: Example of results of DSR with audit logs

ExportItem Id	ACD25409CA01EA4277F96B37DCEA8A79
Item Identity	AAAAAB2EAxGqZhHNm8gAqgAvxFoNAKnU7WPL8LxKr7KK/trQguwAAAHiqw8AAA==
Document ID	1118951
Selected	
Duplicate to Item	
Original Path	henrike@PCdpiaTest.onmicrosoft.com, Primary, a8f34155-b64a-49fb-8a3c-40cb2673f8c5\henrike@PCdpiaTest.onmicrosoft.com (Primary)\Bovenste map van gegevensarchief\Postvak IN
Location	henrike@PCdpiaTest.onmicrosoft.com, Primary, a8f34155-b64a-49fb-8a3c-40cb2673f8c5
Location Name	henrike@PCdpiaTest.onmicrosoft.com
Target Path	
Document Path	
Subject or Title	Floor Terra shared "ziektemelding corona" with you.
Sender or Created by	Floor Terra
Recipients in To line	Henrike van Voorst <henrike@PCdpiaTest.onmicrosoft.com>
Recipients in Cc line	
Recipients in Bcc line	
To – Expanded	
CC – Expanded	
BCC – Expanded	
DG Expansion Result	
Sent	04/05/2021 14:06
Has Attachments	FALSE
Importance	Normal
Is Read	FALSE

Modified by	
Type	Message
Received or Created	04/05/2021 14:06
Modified Date	
Size (KB)	84.377
Decode Status	
Compliance Tag	
Summary	
Preservation Original Url	

The results of this query show that Microsoft, via its own system-generated logs with diagnostic data about the use of the cloud storage and communication services, **collects Content Data from file- and path names of files.**[48] The results of the access request are personal data, because the log files contain directly identifying data such as name, username and email address, as well as specific actions in the online services Teams, SharePoint and OneDrive.

Because these are online processing operations that take place anyway on Microsoft's cloud servers, Microsoft also 'processes' the contents of files and chats on its cloud servers, but admins in the EU can choose to have such Content Data only processed in EU data centres.

The second type of query was not performed for this specific DPIA. In May 2021, Privacy Company did not use this tool, but in September 2021 this tool was used to access the Telemetry Data about a different set of Office 365 applications. Privacy Company was unable to effectively compare the produced data with the captured Telemetry Data from the network traffic. This was due to post-processing by Microsoft of the raw telemetry events. For example, in the produced results Microsoft removed the names of the telemetry events, while these names were instrumental in comparing the collected versus the provided Diagnostic Data. This makes the DSAR for Diagnostic Data unreliable as a transparency tool to verify the scope of the diagnostic data processing.

In reply to the questions raised by SLM Rijk about the (other) test results of the (new) query for system-generated logs, Microsoft explained that there are three reasons why this new query does not produce all observed telemetry events in the network traffic. Microsoft immediately deletes some events, quickly removes the identifiers that would allow for identification, or does not collect any personal data at all with some other events.

"*If a DSR report for system generated logs is initiated, the resulting export will include all records retained by the Microsoft online services that resulted from the user's interactions with the online service and are "tagged" as being "personal data" in our internal records. Given the scope for this report, aspects of the information in RSD*

[48] In a DSR request, Microsoft actively searches for files that are still present on its cloud servers, and in the DSR requests at that time, captures a few fragments from the content of the file. This explains why many fields contain Content Data from the various Word and Excel documents that were shared via Teams from SharePoint Online.

will be in the reported output. However, not all the user's RSD observed at the client side via network observation may be found in a DSR report, for reasons including:

1. *The data may not be retained as personal data – it may not be possible for Microsoft to correlate a retained item solely to the identity provided when the DSR report was initiated. Microsoft designs for data minimalization, both to support the obligations of privacy law and to reduce costs for Microsoft in managing personal data.*

2. *The service may only retain the data for a short period of time, deleting it after the service has performed the requested task, but before the DSR report request was initiated. Again, Microsoft designs for data minimalization, both to support the obligations of privacy law and to reduce costs at Microsoft. This means if there is no utility in the online service functions to retain the information Microsoft does not retain it.*

3. *The data that was sent in the RSD may be instructions related to the connected experience and not personal data. For example, the Microsoft Translator experience sends the source and target languages in RSD so that the cloud powered feature can do what the user wants, but this information is an "instruction" (both in fact and as the GDPR defines such) and is not retained with correlations to a user. Microsoft may retain or compute records about the statistical spread of language elections by users, when the translate experience is invoked, but not in ways that map to the user/data subject.*

4. *The data may be diagnostic data about the connected experience that cannot be correlated to the user provided. For example, diagnostic data telling Microsoft about events preceding an application crash may not be stored with identifiers to the user who was using the application at the time."* [49]

This explanation cannot be verified, due to the lack of event-level information about the browser-generated Telemetry Data, and due to the post-processing removal of event names.

The purpose of using this tool was to get access to the undocumented *Required Service Data*. In view of Microsoft's explanation, no new request was filed during the brief retesting in January 2022.

In sum, the results of the access requests do not give a complete picture of the personal data that Microsoft processes in its logs about the individual use of Teams, SharePoint and OneDrive. Microsoft's explanations about the lack of access to most of the observed telemetry events need to be independently verified.

2.6 Analytical services based on the system-generated log files

Microsoft uses the Diagnostic Data it collects through the use of its Connected Cloud Services to provide several kinds of analytical services. In the last DPIA report for SLM Rijk (published 30 June 2020[50]) about the mobile Office apps and Office for the

[49] E-mail Microsoft to SLM Rijk, 10 December 2021.

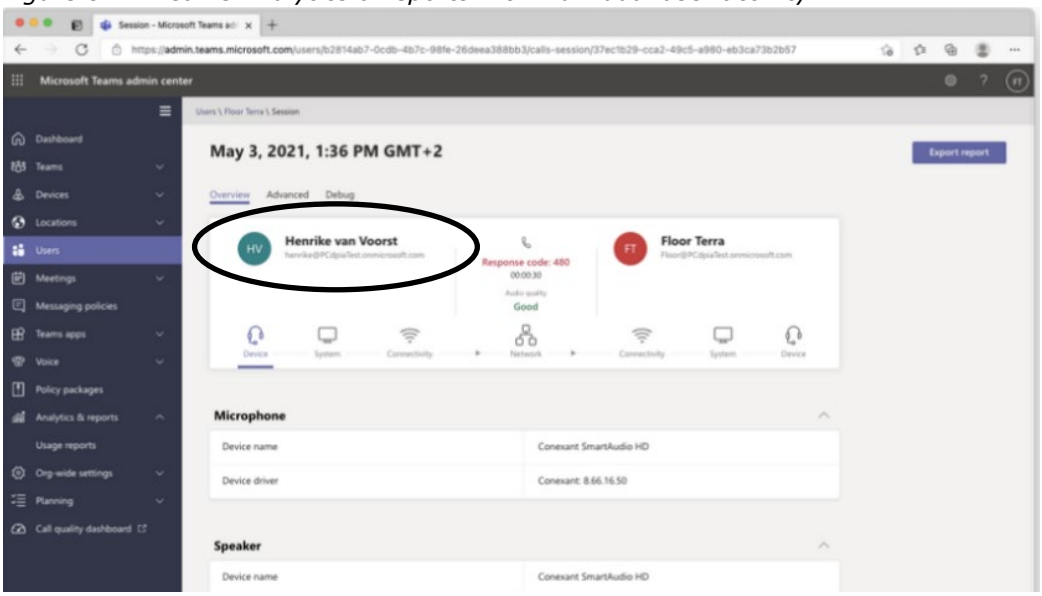
[50] DPIA on Microsoft Office 365 for the Web and mobile Office apps, published 30 June 2020, URL: https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps.

Web, the data processing through MyAnalytics, Delve and through Workplace Analytics was described and analysed. This analysis is not repeated here. Microsoft has since added two new types of analytical reporting: (i) Microsoft Teams Analytics and Reports, and (ii) Microsoft Viva. Additionally, Microsoft also makes analytical data available through the Microsoft 365 admin center, as described in Section 2.4.2 above.

2.6.1 Teams analytics and reports

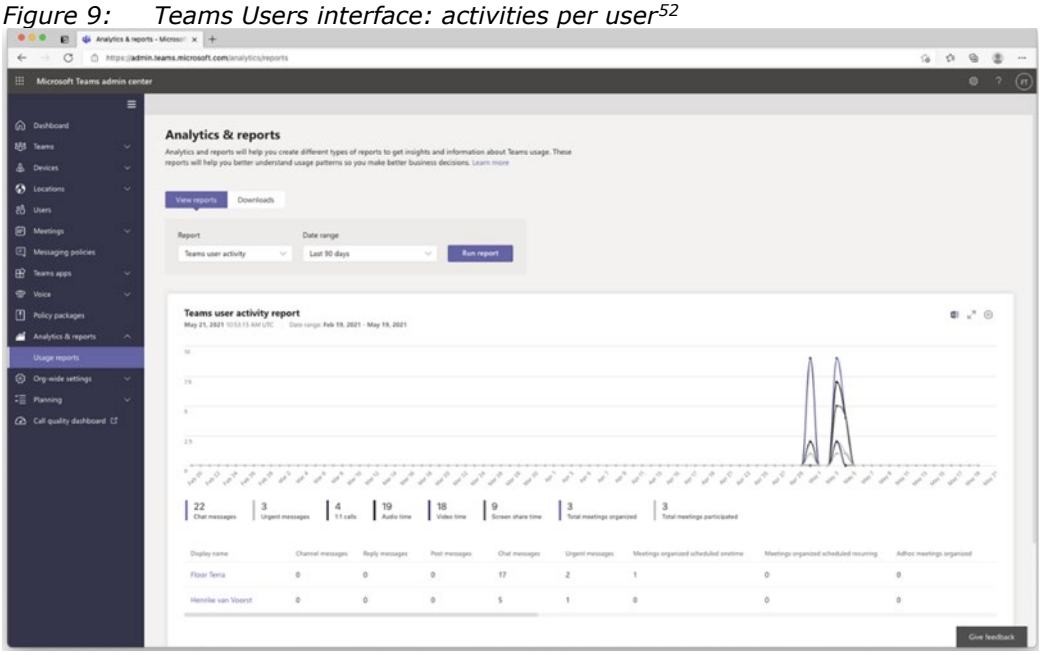
In the admin interface for Teams Analytics & reports, Microsoft shows the activity of individual end-users with their e-mail addresses, how many channel, reply, post and chat messages they sent, how many urgent messages and how many scheduled and ad-hoc meetings they organised. The graphs also show totals for all employees, such as audio and video time, time spent sharing screen and total amounts of calls, and organised meetings.

Figure 8: Teams Analytics & reports with individual user activity [51]



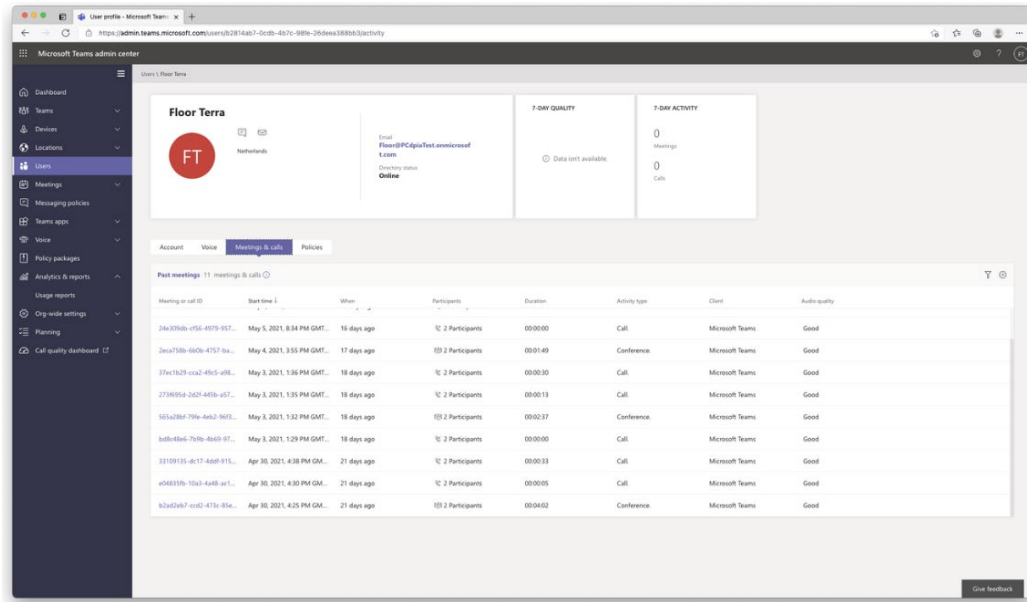
[51] Screenshot made on 24 May 2021 in Privacy Company's test tenant with a Dutch government E5 license.

Figure 9: Teams Users interface: activities per user[52]



An admin can look-up detailed information about the activities of an individual user in a different section of the Microsoft Teams admin center. Figure 9 above shows an example of activities of a test user. It shows the number of past meetings and calls (11), and per meeting the start time and date, duration and number of participants.

Figure 10: Activities per meeting of individual participants, devices and connectivity



In the user interface shown in Figure 10 above, an admin can see minute details of every meeting, with the names of the participants, device and system information for both participants, connectivity and network information, as well as a long list of 'other' data relating to the quality of the connection.

[52] Idem.

By default, all analytic views are turned On by Microsoft, as shown in Figure 11 below. In reply to this DPIA, Microsoft explained that it will not change these default settings.

Admins can customise the view by disabling categories. Such disabling does not mean Microsoft stops collecting the input data for the analytics. Admins do have a privacy choice with regard to the names of the participants: they can replace these identifiers by a pseudonym. This option is discussed in Section 3.1 of this report. Microsoft incorrectly describes this choice as 'making the data anonymous', but also as 'de-identifying information'.

Admins can still look up user activity per named user in the usage files about Teams, OneDrive and SharePoint through the Microsoft 365 admin center, as described in Section 2.4.2 of this report.

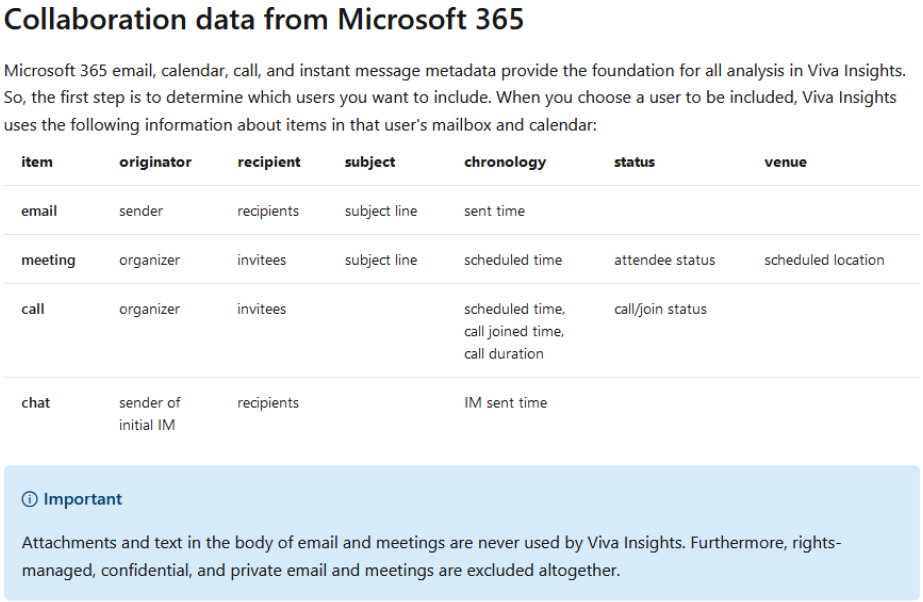
In November 2021, Microsoft made a package available of new combined Analytical services called the Microsoft Viva Suite.[53] Microsoft explains: "*Microsoft Viva builds on the power of Teams and Microsoft 365 to unify the employee experience across four key areas - Engagement, Wellbeing, Learning, and Knowledge in an integrated experience that empowers people to be their best.*"[54]

[53] Microsoft, Microsoft Viva is now generally available to help transform your hybrid work experience, 2 November 2021, URL: https://www.microsoft.com/en-us/microsoft-365/blog/2021/11/02/microsoft-viva-is-now-generally-available-to-help-transform-your-hybrid-work-experience/

[54] Microsoft, Microsoft Viva service description, 22 December 2021, URL: https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-viva-service-description

Figure 11: Default settings in Teams Analytics & reports

Figure 12: Data used for Viva Insights [55]



Collaboration data from Microsoft 365

Microsoft 365 email, calendar, call, and instant message metadata provide the foundation for all analysis in Viva Insights. So, the first step is to determine which users you want to include. When you choose a user to be included, Viva Insights uses the following information about items in that user's mailbox and calendar:

item	originator	recipient	subject	chronology	status	venue
email	sender	recipients	subject line	sent time		
meeting	organizer	invitees	subject line	scheduled time	attendee status	scheduled location
call	organizer	invitees		scheduled time, call joined time, call duration	call/join status	
chat	sender of initial IM	recipients		IM sent time		

Important

Attachments and text in the body of email and meetings are never used by Viva Insights. Furthermore, rights-managed, confidential, and private email and meetings are excluded altogether.

The four analytical modules are partially based on existing analytic tools. Viva Insights builds on MyAnalytics and Workplace Analytics. The tool provides both individual and group insights. Microsoft's data sources are shown in Figure 12 above. Viva also includes details about chat and call history from Teams and Skype for Business. Viva will soon also include an existing tool recently acquired by Microsoft (Ally.io) in 2022, for performance management. "*The shift to hybrid has made it more challenging to keep every leader, team and individual aligned and moving to the same rhythm. Ally.io helps give everyone in the organization visibility and clarity into the entire work process, connecting everyday work to the company's strategic objectives.*"[56]

Microsoft has explained that for Viva the default setting is privacy friendly: administrators must enable these services, while end users can opt-out, even if the administrator has enabled the service. These privacy choices are discussed in Section 3 of this DPIA.

2.7 Types of personal data and data subjects

As emphasized above**,** this DPIA cannot provide the required limitative overview of the different kinds of personal data that will be processed by the Office Diagnostic Data. However, this report does provide some assistance to the government organisations about these categories, to help them decide about the actual installation and settings based on an inventory of the types of personal data that are factually processed in their specific organisation.

[55] Microsoft explains that administrators have full control over the data used for Viva Insights. See: You control the data that Viva Insights uses, 22 December 2021, URL: https://docs.microsoft.com/nl-nl/viva/insights/privacy/privacy-and-data-access#you-control-the-data-that-viva-insights-uses

[56] Microsoft, 7 October 2021, Microsoft acquires Ally.io to improve employee experience by aligning people's work with team goals and company mission, URL: https://blogs.microsoft.com/blog/2021/10/07/microsoft-acquires-ally-io-to-improve-employee-experience-by-aligning-peoples-work-with-team-goals-and-company-mission/

2.7.1 Categories of personal data

Generally speaking, users and employers can process all kinds of personal data in Office. These products can be used for many different purposes by many different organisations. Absent a comprehensive documentation and publicly available policy rules governing the types of data that can be stored by Microsoft as Diagnostic Data, it has to be assumed that Office Diagnostic Data may include all categories of personal data. Some kinds of data deserve extra attention. As a result of the negotiations with SLM Rijk in May 2019, Microsoft offers an appendix to the Standard Contractual Clauses with a long list of possible categories of data. Government organisations can compare this list with the overview of personal data in their data processing inventory.

Classified Information

Depending on the capacity in which Dutch government employees work, they may process confidential government information or state secrets (Classified Information). The Dutch government defines four classes of Classified Information, ranging from confidential within a department (DEP-V) to top secret.[57]

If data contain personal data, according to the governmental security standard BIO, security measures described for level BBN2 are mandatory. If an organisation applies BBN2, they can process the first level of classified information (DEP-V). According to national policy intentions with regard to the use of cloud services by Dutch government organisations, from a security point of view, data protected at BBN2 level may be stored in a public cloud, subject to additional conditions. The security level BBN2 does not match with the risks levels for personal data in the GDPR.

Classified Information is not a separate category of data in the GDPR or other legislation concerning personal data. However, information processed by the government that is qualified as Classified Information, regardless of whether it qualifies as personal data, must be protected by special safeguards. The processing of this information may also have a privacy impact if such information relates to a specific individual. If the personal data of a government or university employee, such as his email address at the domain of his employer, or a unique device identifier, reveals that this person works with Classified Information, the impact on the private life of this employee may be higher than if that employee would only process 'regular' personal data. Unauthorised use of Classified Information could for example lead to a higher risk of being targeted for social engineering, spear phishing and/or blackmailing.

If government organisations or universities use Microsoft's OneDrive to store audio and video recordings and the chat history in Teams, they have to be aware that the information stored on these (EU-based) cloud servers may include Classified Information from and about employees, including information which employees regularly discuss or share confidential data. Unauthorised use of this information could for example lead to a higher risk of being targeted for social engineering, spear phishing and/or blackmailing.

If government organisations use SharePoint Online or OneDrive for Business, they have to be aware that the information stored on Microsofts cloud computers may include confidential information from and about government employees, including

[57] Amongst others, the categories of classified information are defined in the Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI).

information which employees regularly access, send, or receive labelled information. Such metadata may end up in system generated server logs.

Personal data of a sensitive nature

Some 'normal' personal data have to be processed with extra care, due to their sensitive nature. Examples of such sensitive data are financial data, traffic and location data. Both the contents of communication as well as the metadata about who communicates with whom, are of a similar sensitive nature. The contents of communication are specifically protected as a fundamental right, but metadata deserve a high level of protection as well. This will be explained in more detail in Section 16 of this report.

The sensitivity is related to the level of risk for the data subjects in case the confidentiality of the data is breached. Risks may vary between slight embarrassment, shame, a chilling effect preventing a data subject from seeking further assistance from that government organisation or university or an employee or student from effective communication, blackmailing, discrimination, exclusion, identity and/or financial fraud and even a risk of stalking. Employees and students may experience a chilling effect as a result of the monitoring of their behavioural data. The audit logs for example could be used by the employer to reconstruct a pattern of the hours worked with the different applications. Such monitoring could lead to a negative performance assessment, if not specifically excluded in a workers Privacy Statement. Similarly, analytical tools such as Teams Analytics & reports and the Activity Reports in the Microsoft 365 admin center provide very detailed insights in the behaviour of groups of employees and students. Although Microsoft aims to provide pseudonymised insights relating to five people or more in the activity reports, this is not the case for the usage data about Teams.

It is likely that many government and university employees process personal data of a sensitive nature on a daily basis with the online storage and communication tools included in the Office 365 license. Personal data of a sensitive nature may be included in snippets of content (such as the line preceding and following a word) that may be included in system generated event logs about the opening or saving of files in SharePoint or OneDrive.

Special categories of personal data

Special categories of personal data are especially protected by the GDPR. According to Article 9 (1) GDPR, personal information falling into special categories of data is any:

> *"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".*

With special categories of data, the principle is one of prohibition: these data may *not* be processed. The law contains specific exceptions to this rule, however, for instance when the data subject has explicitly consented to the processing, or when data has been made public by the data subject, or when processing is necessary for the data subject to exercise legal claims.[58]

[58] These specific exceptions lifting the ban on the processing are listed in Article 9(2) under a, e, and f of the GDPR.

Since government organisations such as the police and the judiciary work with the Office software, and universities conduct for example medical or psychological research, it cannot be excluded that the Diagnostic Data may contain information on special categories of data in the file and pathnames.

2.7.2 Categories of data subjects

Generally speaking, the different kinds of data subjects that may be affected by the Diagnostic Data processing, can be distinguished in three groups, namely: employees and students that use the applications for work or study, guest users and miscellaneous. Microsofts appendix to the SCC also contains a list of possible data subjects. Government organisations and universities can compare this list with the overview of data subjects in their data processing inventory.

Employees and students

The users of the Office software are employees of a governmental organisation or university, including contractors and (temporary) workers, and the students.

Their names and other personal information are processed in connection with the documents they create and store in OneDrive or SharePoint, and frequently carry their (last) name. Their names and other personal information are also attached to the conferencing, chatting and calling activities they perform in Teams.

Apart from the information generated by the employees and students themselves, employees are also data subjects in information generated by other employees and students. For instance, when they are mentioned in a discussion on Teams, or in a document shared via OneDrive.

As the uses of the Office software are so varied, it is impossible to give an exhaustive list.

Guest users

Teams and OneDrive are designed to make it easy to share information internally and externally in a secure way. Guest users can be invited to share a Team discussion, or access files shared in OneDrive. This means their name and email address, or alias becomes part of the Diagnostic Data processed on Microsoft’s cloud servers, as well as the times they interacted with the university or government organisation. Microsoft has ensured SLM Rijk in November 2020 that all data relating to guest users are processed according to the negotiated privacy amendment if they are invited as guest user by a government organisation or university. However, if they participate from their own consumer Teams client, be it through a browser, on their mobile or desktop, it appears the consumer privacy conditions continue to apply.

Miscellaneous other data subjects

Besides employees/students and guest users, there is a third miscellaneous group of individuals whose personal data may be processed in files and pathnames included in the Diagnostic Data generated by the use of OneDrive and SharePoint.

The bottom line is that there are no limits to the categories of data subjects whose data may be processed in Diagnostic Data generated by the use of Office software in normal use conditions by employees of the Dutch government.

3. Privacy controls

This section discusses the different privacy controls for end-users and administrators to minimise the processing of data about the individual use of Teams, OneDrive , SharePoint and the Azure AD.

The purposes for which Microsoft collects the Diagnostic Data are described in Section 4 of this report.

3.1 Privacy controls system administrators

This section describes nine different privacy controls system administrators can exercise:

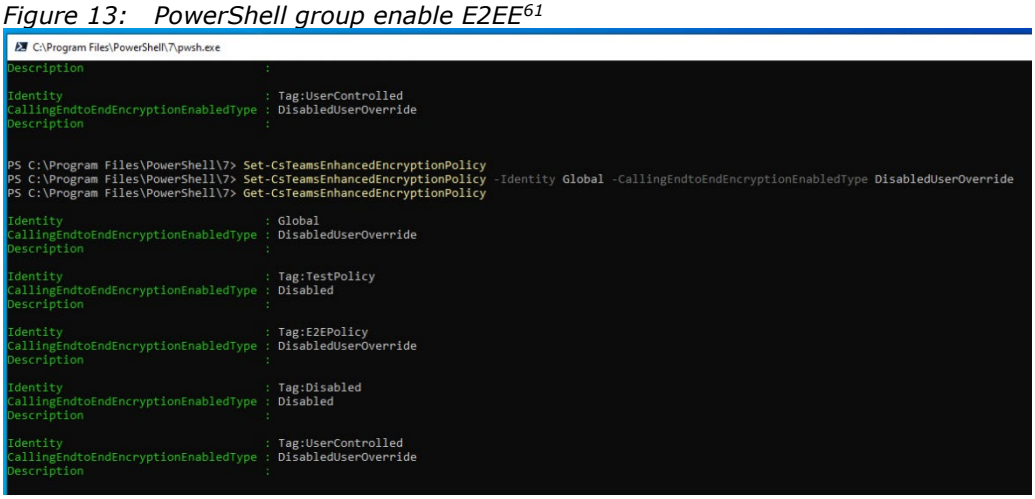
1. Enabling end-to-end-encryption
2. Enabling Customer Key, Customer Lockbox or Double Key Encryption
3. Minimising the telemetry level
4. Blocking the use of Controller Connected Experiences
5. Blocking access to non-Microsoft apps in the Teams store
6. Blocking the use of Giphy in Teams
7. Forcing users to accept the organisation's privacy rules through Conditional Access rules in the Azure AD
8. Pseudonymising usernames in Teams Analytics & reports
9. Enabling Microsoft Viva

These nine options are discussed in more detail below.

3.1.1 Enabling end-to-end encryption

Administrators can enable users to opt-in to E2EE in the Teams admin center.[59] This option is currently not available as standard choice, but can be activated with a group policy in PowerShell.[60]

Figure 13: PowerShell group enable E2EE[61]



As shown in Figure 14 below, Microsoft does not yet offer E2EE for scheduled online meetings and meetings with multiple participants.

[59] Admins can sign in to: https://admin.microsoft.com/Adminportal/Home

[60] Tested by Privacy Company on 14 February 2022 in a Dutch government E5 license.

[61] Idem.

Figure 14: Microsoft Q&A about E2EE[62]

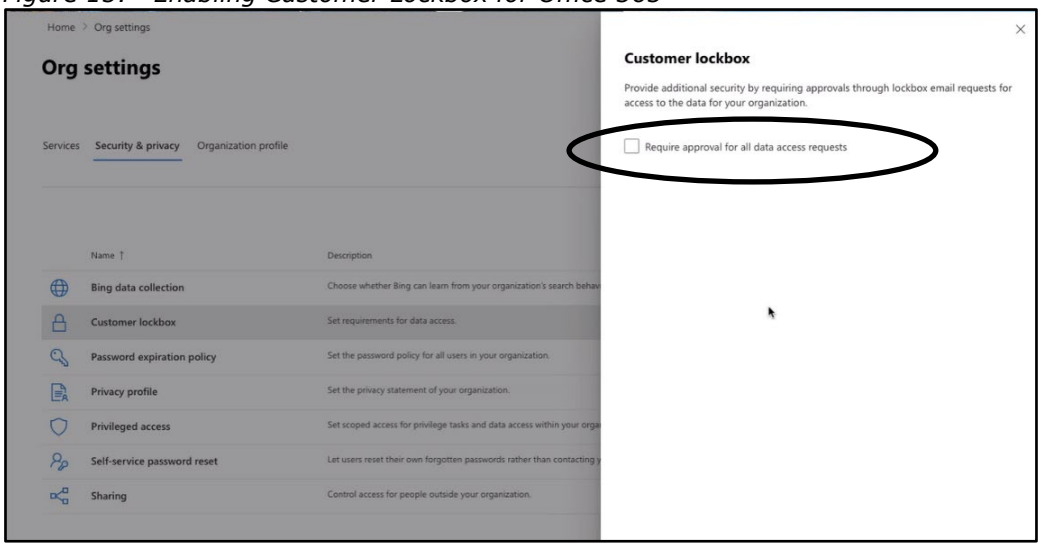
Can I use E2EE for group meetings and calls?

Not yet. Initially E2EE will be available only for one-on-one Teams calls. After gathering customer feedback to understand how the feature addresses their compliance needs and obligations, we will work to bring E2EE capabilities to online meetings.

3.1.2 *Enabling Customer Key, Customer Lockbox or Double Key Encryption*

Admins can enable an extra level of protection for data stored in Exchange Online (includes Team data), SharePoint and OneDrive, by turning On Customer Lockbox in the main Microsoft 365 admin portal.[63] When enabled, the customer receives a permission request to decrypt every time a Microsoft engineer needs to access the data. They can also choose to add an extra level of encryption with Customer Key.

Figure 15: Enabling Customer Lockbox for Office 365[64]



3.1.3 Minimising the telemetry level

Since the spring of 2019 Microsoft distinguishes between three telemetry levels in the Enterprise versions of Office 365:

1. Optional
2. Required

---

[62] Microsoft, Can I use E2EE for group meetings and calls?, Undated, last visited 28 January 2022, URL: https://support.microsoft.com/en-gb/office/use-end-to-end-encryption-for-teams-calls-1274b4d2-b5c5-4b24-a376-606fa6728a90#ID0EBD=Desktop

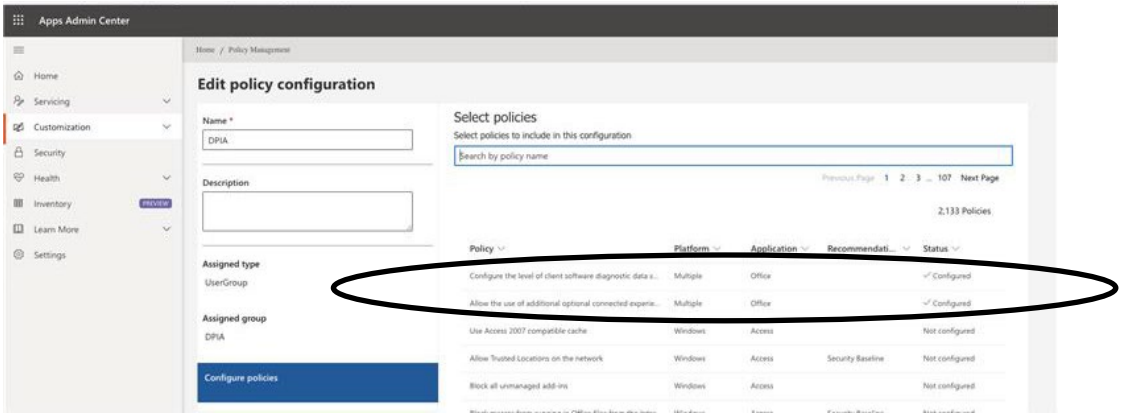
[63] Microsoft, Customer Lockbox in Office 365, 26 January 2022, URL: https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide

[64] Microsoft, Turn Customer Lockbox requests on or off, 26 January 2021, URL: https://docs.microsoft.com/en-gb/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide#turn-customer-lockbox-requests-on-or-off

3. Neither[65]

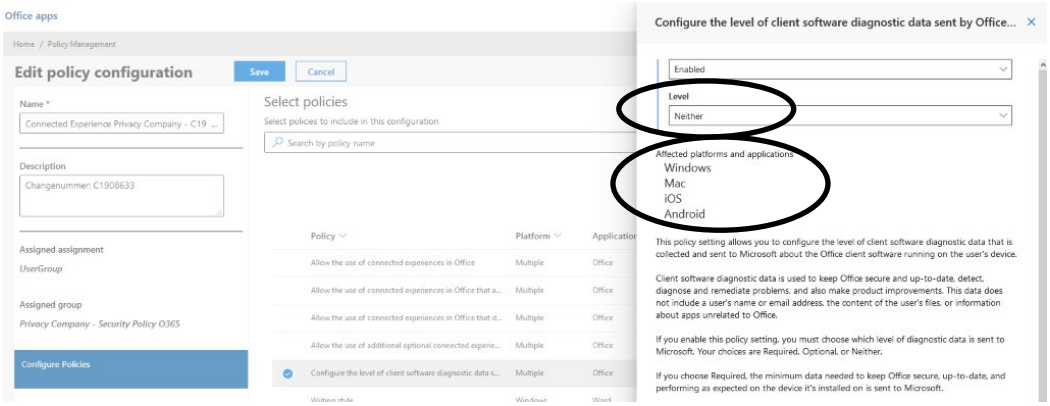
Since the fall of 2020, this privacy control is also available for the telemetry events from the OneDrive, Outlook and Teams apps and from Office for the Web. See Figures 16 and 17 below. Admins should be aware of the inconsistency in the activation of these privacy choices: they must first enable the 'configuration' of the diagnostic data and the connected experiences before they can choose the minimum level in the next step.

Figure 16: Admin console: set policies for Diagnostic Data



As shown in Figure 16 below, in the test environment the telemetry level for the tested apps was set to the lowest level: 'Neither'.

Figure 17: Configuration of telemetry level to Neither

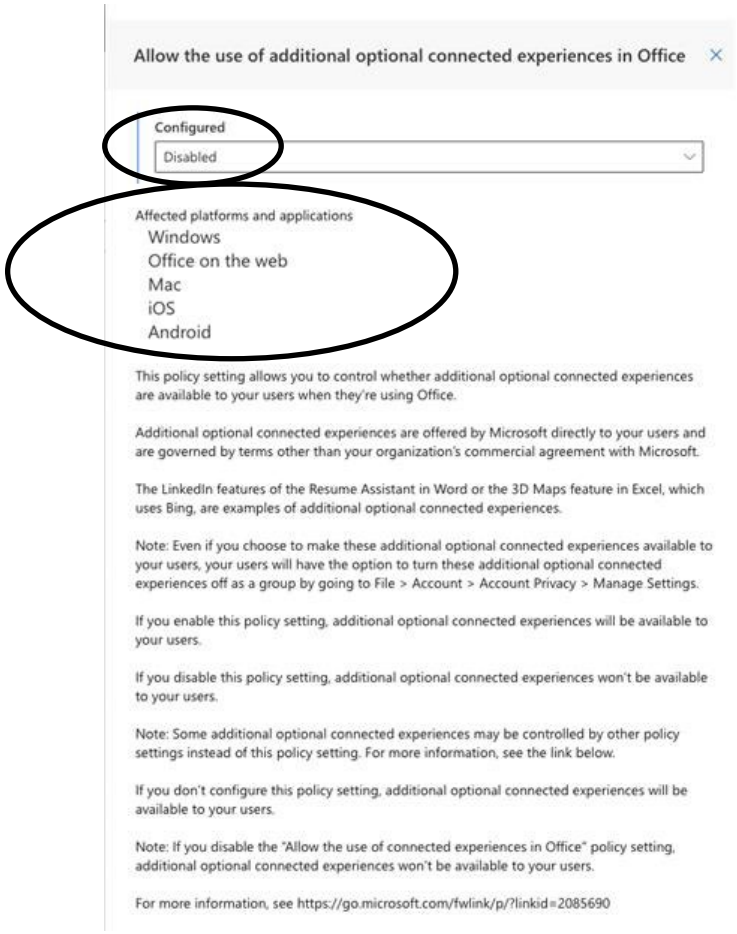


3.1.4 *Blocking Controller Connected Experiences*

As shown in Figure 18 below, admins can switch off the Controller Connected Experiences on all platforms, for all the Office 365 services. Microsoft calls these services 'Additional Optional Connected Experiences', even though they are enabled by default.

[65] Microsoft, Required Diagnostic Data for Office, 20 January 2022, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/required-diagnostic-data

Figure 18: Admin console: Controller Connected Experiences disabled



3.1.5 *Blocking access to non-Microsoft apps in Teams*

Microsoft has explained that admins can disable access to non-Microsoft apps in the Teams store, in the Microsoft Teams admin center, on the *Manage apps* page, by selecting *Org-wide app settings*. *"Administrators that do not wish their users to access app descriptions that contain links to YouTube videos can either disable all apps, or disable access to just the apps that include videos embedded in the app descriptions, such as the Polly app."*[66]

Privacy Company verified that if this setting is effectuated, end users indeed only see Microsoft apps in the Teams store, as shown in Figure 20 below.

[66] Reply Microsoft to SLM Rijk 27 June 2021. See also: Microsoft, Manage org-wide app settings, 27 January 2022, URL: https://docs.microsoft.com/nl-nl/microsoftteams/manage-apps#manage-org-wide-app-settings

Figure 19: Admin menu to block access to non-Microsoft apps in Teams[67]

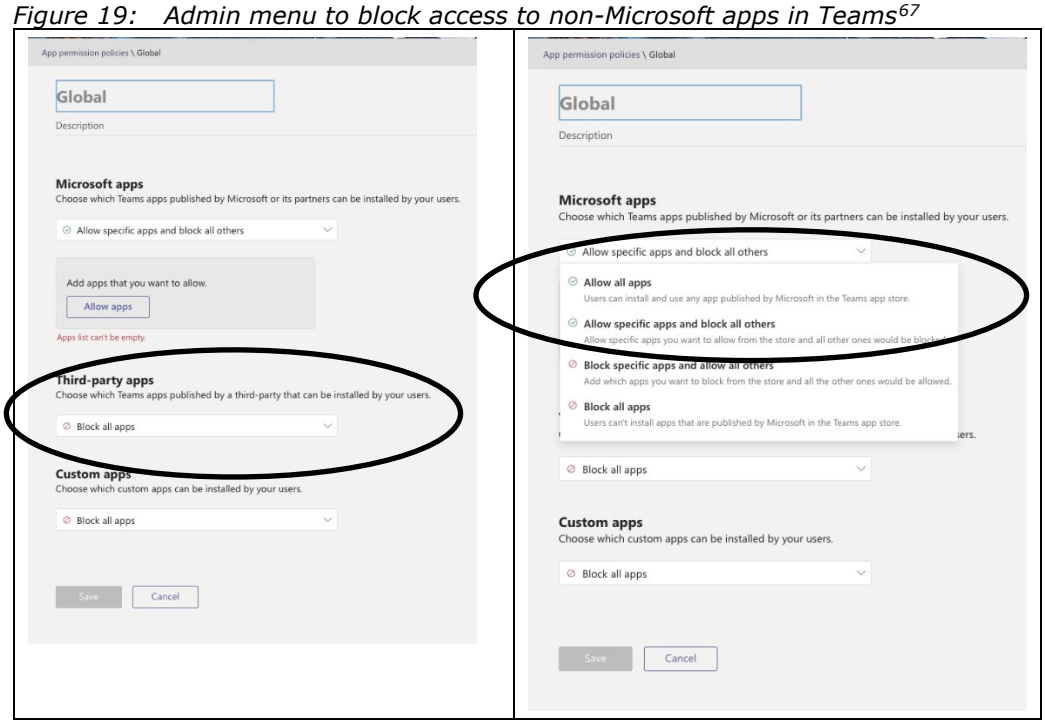
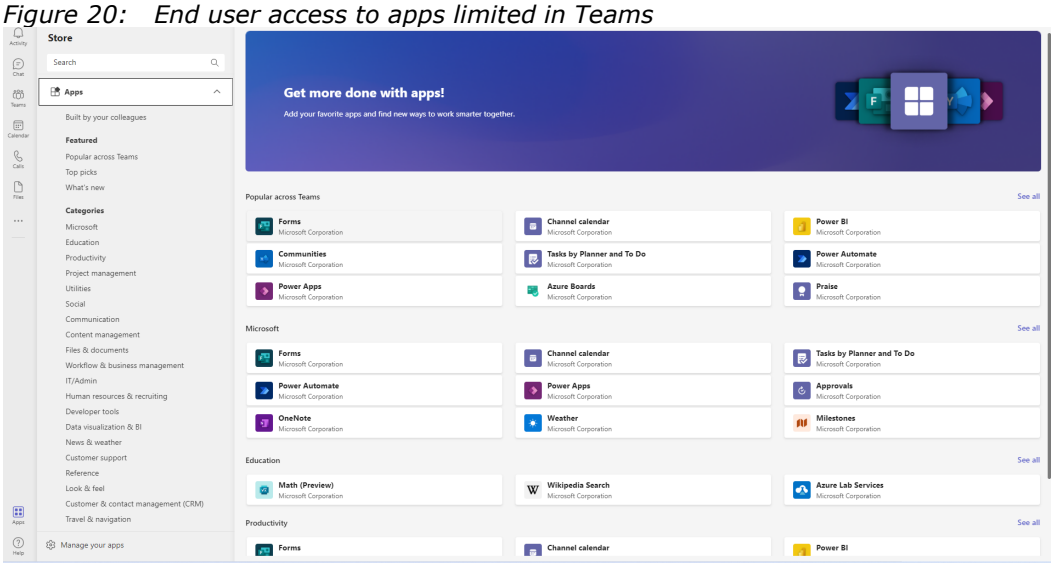


Figure 20: End user access to apps limited in Teams

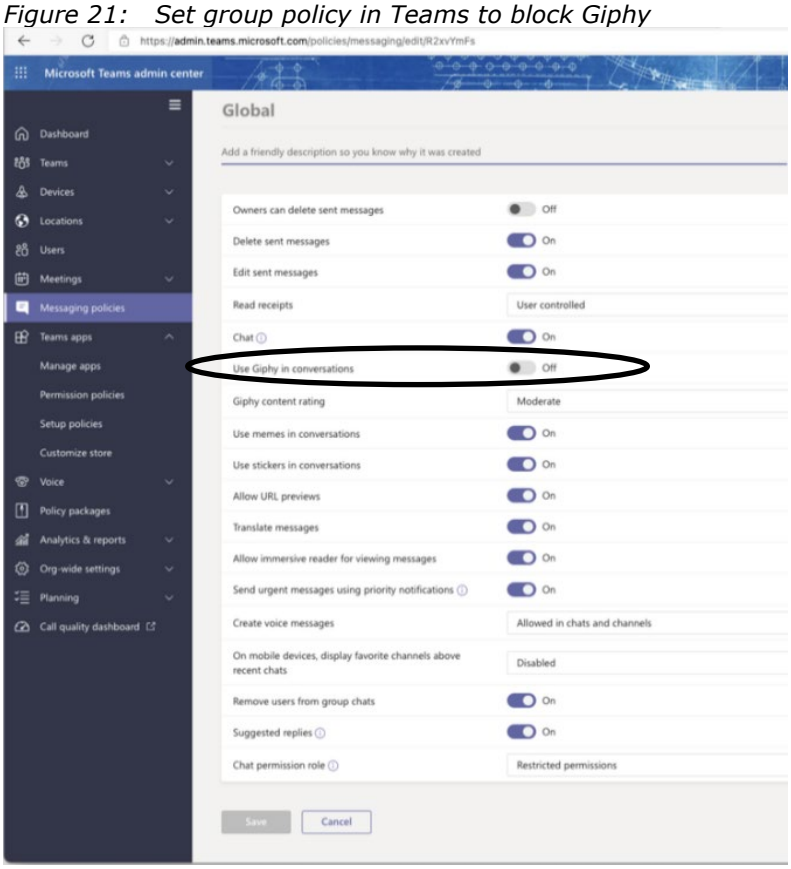


3.1.6 *Blocking the use of Giphy in Teams*

The use of Giphy is not (yet) part of the Controller Connected Experiences. Admins have to select a separate group policy in Teams to disable this functionality. As shown in Appendix 1, this functionality does not prevent guest users from including Giphy pictures in their conversations on Teams. This in turn causes personal data from employees and students to be sent to Giphy.

[67] New screenshot made on 16 February 2022.

Figure 21: Set group policy in Teams to block Giphy



3.1.7 *Enforcing acceptance of organisational privacy rules through Azure AD*

Microsoft has recently added a new privacy choice to the Azure Active Directory. As part of the Conditional Access options, the Azure AD can be instructed to force end users, including guest users, to accept organizational policies.[68] Conditional Access policies are enforced after first-factor authentication is completed. Admins can thus enforce awareness of relevant privacy rules amongst employees, students and guest users.

Microsoft explains that Enterprise and Edu customers require an Azure AD Premium P1 license to use the feature. In the test tenant created for this DPIA, an E5 government license, this feature was not available.

3.1.8 *Option to pseudonymise identifiable user data in Teams Analytics & reports*

An admin can choose to pseudonymise the names and e-mail addresses of end-users in the Teams Analytics & reports, and in the users reports. Microsoft offers this option in the Microsoft 365 admin center, under 'Services', 'Reports'.

In its public documentation, Microsoft incorrectly calls this process 'Make the user specific data anonymous. See Figure 22 below.

[68] Microsoft, What is Conditional Access? 27 January 2021, URL: https://docs.microsoft.com/en-gb/azure/active-directory/conditional-access/overview

Figure 22: Microsoft's use of the word 'anonymous'

Make the user specific data anonymous

To make the data in Teams user activity and Teams device usage report anonymous, you have to be a global administrator. This will hide identifiable information such as display name, email and AAD ID in reports and their exports.

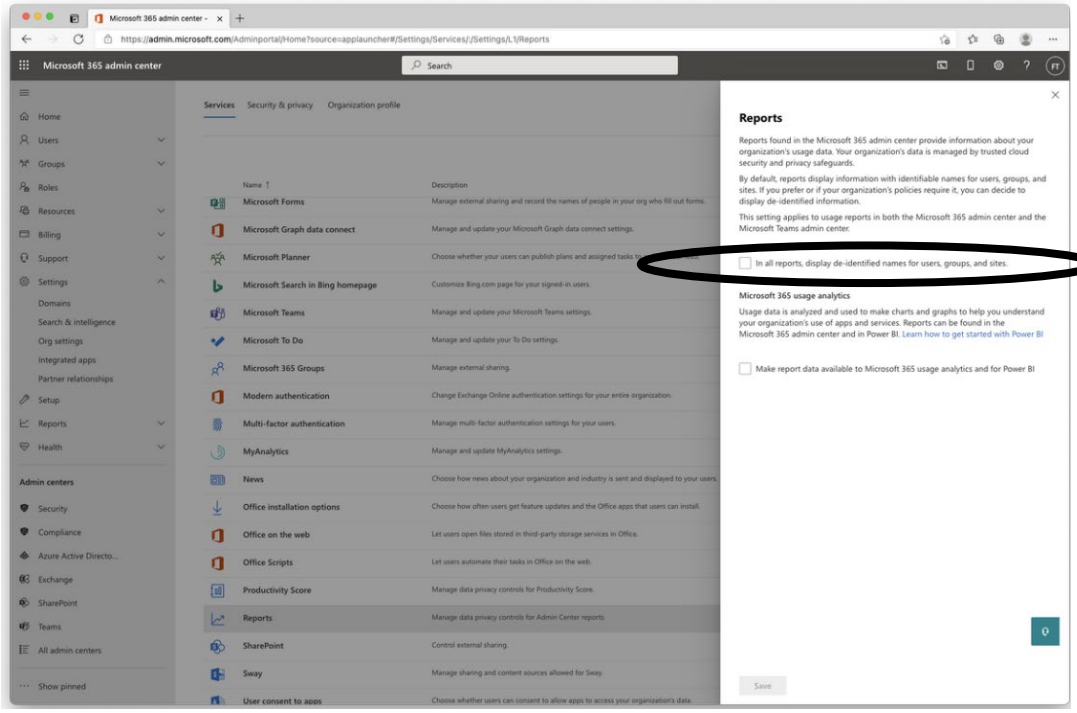
1. In Microsoft 365 admin center, go to the **Settings** > **Org Settings**, and under **Services** tab, choose **Reports**.
2. Select **Reports**, and then choose to **Display anonymous identifiers**. This setting gets applied both to the usage reports in Microsoft 365 admin center as well as Teams admin center.
3. Select **Save changes**.

Note

Enabling this setting will de-identify information in **Teams user activity report** and **Teams device usage report** reports. It will not affect other usage reports available in Teams admin center.

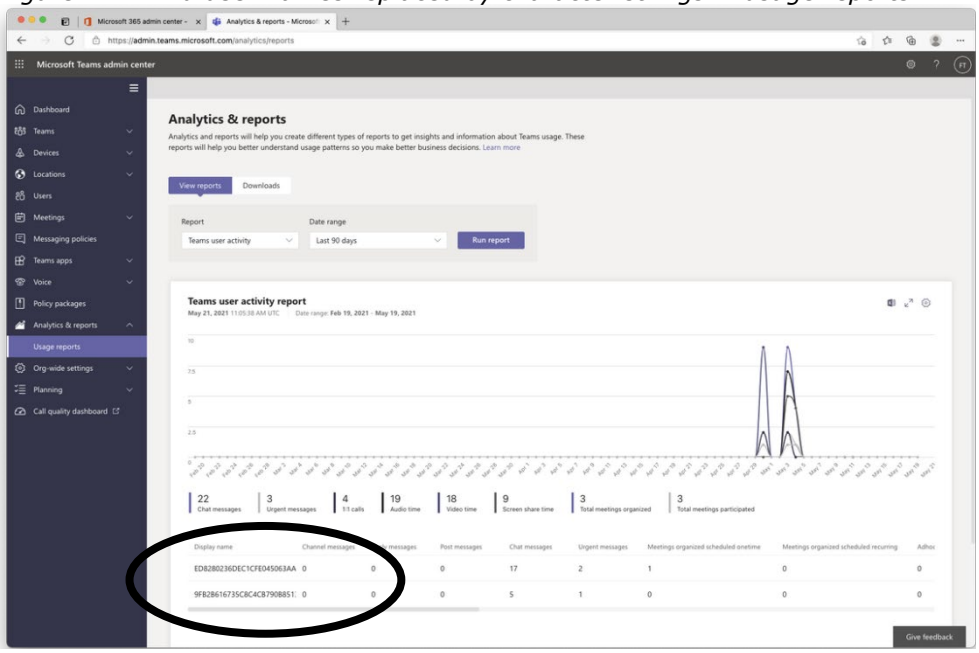
Microsoft describes this choice as '*display de-identified names for users, groups and sites*.'

Figure 23: End user pseudonymisation option in Reports



Enabling this option effectively results in pseudonymisation of the directly identifiable usernames in the usage report.

Figure 24: End user names replaced by character strings in usage reports



3.1.9 *Option to enable Microsoft Viva*

Microsoft Viva's default configuration requires an administrator to explicitly enable the service; the individual user has the option to opt-out.

Additional details can be found below; this documentation describes the actions an administrator has to work through to enable the service, as well the opt-out choice for users. Personal Insights data is stored in the Exchange Online mailbox of the user.

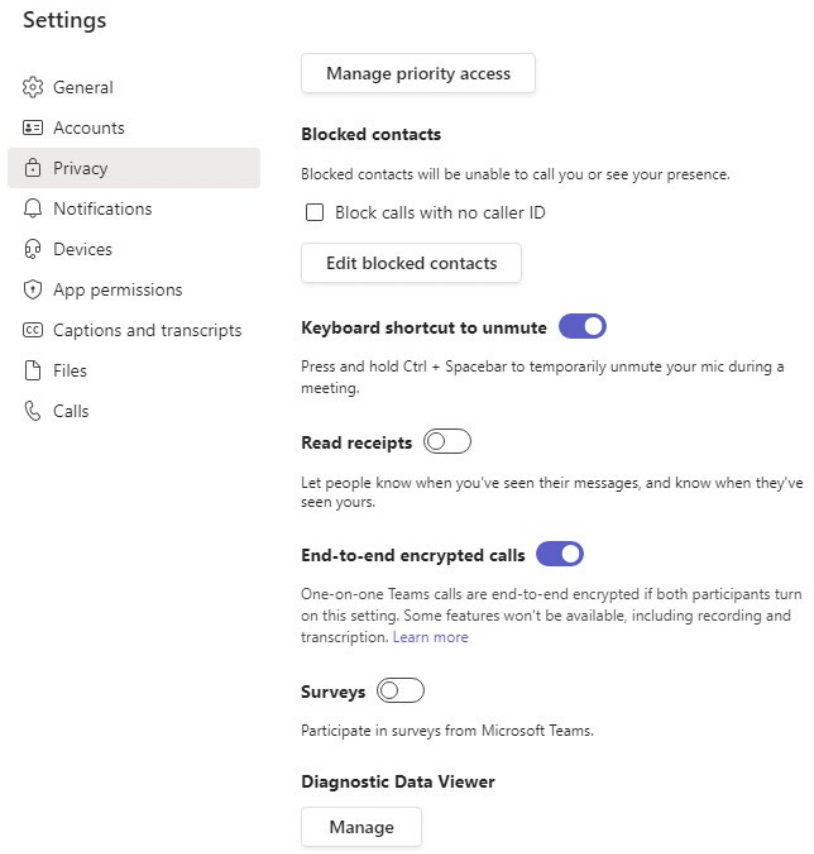
3.2 Privacy controls end users

3.2.1 *Enable end-to-end encryption for 1-on-1 calls*

Once administrators can and have enabled the use of E2EE, end users must still actively turn this option on.[69] They should navigate to the 'Settings' in their Teams client, and select the box 'End-to-end encrypted calls'.

[69] Microsoft, Use end-to-end encryption for Teams calls, undated, last visited 28 January 2022, URL: https://support.microsoft.com/en-gb/office/use-end-to-end-encryption-for-teams-calls-1274b4d2-b5c5-4b24-a376-606fa6728a90#ID0EBD=Desktop

Figure 25: End user option to enable E2EE[70]



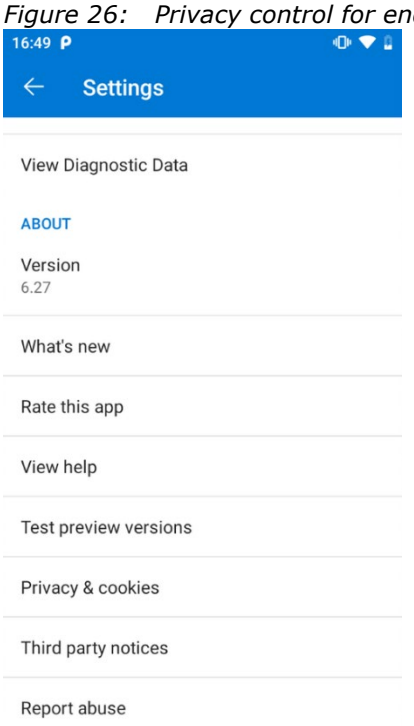
3.2.2 *Enable Data Viewer Tool*

End users can enable the Data Viewer tool for Teams and OneDrive on their mobile devices (both Android and iOS), and for Teams also on Windows and MacOS desktops.

If the system administrator does not centrally prohibit the use of Controller Connected Experiences, end users can opt-in to the use of these Controller services, as shown in Figure 26 below.

[70] Screenshot made by Privacy Company on 14 February 2022 in the E5 government license. E2EE was enabled, privacy unfriendly options such as 'read receipts' and 'surveys' were disabled.

Figure 26: Privacy control for end users in Android: turning on Data Viewer tool



4. Purposes of the processing

Government organisations and universities can use the Diagnostic Data about Teams, OneDrive, SharePoint and the Azure AD for security and compliance purposes, for example to detect and mitigate security incidents and to control the access to personal data processed through the online cloud storage. Use of the cloud storage allows organisations to offer a reliable service that is accessible from multiple locations. These government and university interests in the use of Office 365 are described in section 6.1 of this report.

Depending on Microsoft's role as processor or as controller, there are two different groups of purposes for which Microsoft processes personal data:

1. Purposes for the processing of the Diagnostic Data from its cloud storage and communication services.

2. Purposes for the processing of telemetry events from the installed apps and browser accessible versions of Teams, OneDrive and SharePoint.

4.1 Purposes Diagnostic Data generated on cloud servers

On the basis of the OST and the DPA (as adjusted by the Dutch government's privacy amendment), Microsoft considers itself to be a data processor for the processing of all personal data that it processes through the use of Teams, OneDrive, SharePoint and the Azure AD after a user is signed in with a school or work account, including all Diagnostic Data.

The privacy amendment stipulates that Microsoft may only process the personal data that it obtains from, about, or via the use of its Online Services for three authorised

purposes, and only when proportional. These purposes are: (1) to provide and improve the service, (2) to keep the service up-to-date and (3) secure.

The Dutch government and Microsoft have also agreed that Microsoft may never process for the following purposes:

1. Data analytics

2. Profiling

3. Advertising or similar commercial purposes, including targeted on-screen recommendations for Microsoft products or services that the customer does not use

4. Market research aimed at developing new functionalities, services or products.

In March 2021, SLM Rijk published the results of the first audit on Microsoft's compliance with these processing limitations, in particular the prohibition on profiling.[71]

4.2 Purposes Telemetry Data generated on user devices and browser

As part of its ongoing compliance commitments, Microsoft has clarified its role as data processor for the Telemetry Data from the mobile Office apps and the browser-accessible applications (Office for the Web). In its new universal license terms for Online Services[72], Microsoft explains it may only process the Telemetry Data for the (three authorised) purposes defined in the Data Protection Addendum for its Online Services.

"*Some Online Services may require, or may be enhanced by, the installation of local software (e.g., agents, device management applications) ("Apps"). The Apps may collect Diagnostic Data (as defined in the DPA) about the use and performance of the Apps, which may be transmitted to Microsoft, to the extent any Personal Data is contained therein, and used for the purposes described in the DPA.*"[73]

The reference to the DPA for the browser-accessible applications implies that Microsoft (only) processes these Telemetry Data for the three authorised purposes.

Microsoft similarly explains the purpose limitation for the mobile Office apps in the Product Terms for Microsoft 365 Applications.[74]

---

[71] See the website of SLM Rijk, for the full audit reports in Dutch and English. Memo from SLM Rijk, https://slmmicrosoftrijk.nl/wp-content/uploads/2021/04/20210408-Memo-Audit-EY-Microsoft-2020-ENG-pdf.pdf. Summary EY of audit report in English: https://slmmicrosoftrijk.nl/wp-content/uploads/2021/04/REQ5267448-B-MinJen-V-Summary-report-Profiling-restrictions-Microsoft-final-wg-versie.pdf

[72] Microsoft, Universal License Terms, For Online Services, URL: https://www.microsoft.com/licensing/terms/product/ForOnlineServices/EES

[73] Idem, under 'Validation, Automatic Updates, and Collection for Software'.

[74] Microsoft 365 Applications, Service Specific Terms, URL: https://www.microsoft.com/licensing/terms/productoffering/Microsoft365Applications/MPSA and

"*When versions of Microsoft Word, Excel, PowerPoint, Outlook, OneDrive, and Teams applications for mobile devices ("M365 Mobile Applications") are used with a work or school account to access Online Services governed by these terms, the terms that govern the relevant Online Service apply to that use of the M365 Mobile Applications."*[75]

4.3 Purposes Microsoft and third parties as data controllers

In reply to the technical findings from May 2021, Microsoft has improved its software or provided instructions how admins can prevent certain data sharing with third parties.

In spite of the contractual purpose limitation for all Diagnostic Data, as explained in the two sections above, Microsoft shared some personal data with itself (Bing) as a data controller. Microsoft allowed SharePoint – when accessed in the browser - to send personal data to its search engine Bing, even if the admin has blocked access to all Controller Connected Experiences. Microsoft has committed to completely eliminate such traffic to Bing by July 2022, when a customer has disabled the Controller Connected Experiences. As explained in Section 2.3.2, as a controller Microsoft permits itself contractually to process the personal data for all seventeen purposes from its (consumer) privacy policy (see also Section 5.4.2 of this report). This includes the display of personalised advertising. See the previous DPIA on Office 365 for the Web and mobile Office apps, as published 30 June 2020, for a full listing of these data controller purposes.[76]

Microsoft still allows some Support pages to share data with the US Content Delivery Network Cloudflare. Absent a data subprocessor agreement with Microsoft and agreement from EU Enterprise and Education Customers, the purposes for which Cloudflare may process the personal data about the website visitors is unknown.

Microsoft has clarified that admins can disable the access to external apps in Teams for end users. This is an important measure to prevent traffic to processing for unknown purposes by third parties via the thumbnails and app descriptions in this Teams store. Additionally, Microsoft has ensured that the group policy to prevent the use of the images database Giphy in Teams also prevents guest users from uploading Giphy-pictures. Prior to this improvement, personal data could still be shared with Giphy, and processed for the purposes that Giphy determines as independent data controller.

5. (Joint) controller or processor

5.1 Definitions

Article 4 of the GDPR contains definitions of the different roles of parties involved in the processing of data: (joint) controller, processor and subprocessor.

https://www.microsoft.com/licensing/terms/productoffering/Microsoft365Applications/MPSA#ServiceSpecificTerms.

[75] Idem, under 'Smartphone and Tablet Devices'.

[76] DPIA on Microsoft Office 365 for the Web and mobile Office apps, published 30 June 2020, URL: https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps.

Article 4(7) of the GDPR defines the (joint) controller as:

"*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*"

The GDPR stipulates in Article 26 that joint controllers must determine their roles and responsibilities, especially towards data subjects, in a transparent agreement.

The GDPR stipulates in Article 4(8) that a processor may only process data on behalf of a data controller. *'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

Article 28 GDPR determines that the obligations of processors towards the controllers for whom they process data. Article 28 GDPR contains 8 specific obligations for the processor, such as that it may only process personal data in accordance with documented instructions from the controller, and that it must, for example, cooperate with audits. It follows from Article 28(4) GDPR that a processor may use subprocessors to perform specific tasks for the data controller.

5.2 Contractual arrangements between SLM Rijk, SURF and Microsoft

Under the privacy amendment with SLM Rijk and SURF, Microsoft is contractually bound to process personal data received, collected, generated or derived in connection with the Online Service Terms only as a data processor, except for certain limited legitimate business purposes and the Controller Connected Experiences, for which Microsoft is the controller.

Microsoft provides its main legal privacy guarantees through its Online Service Terms (OST)[77] and the Data Protection Addendum (DPA).[78] Starting in March 2021, Microsoft no longer offers an integrated Word document of its OST. Microsoft only publishes two skeleton sets of universal license terms (for Online Services and for all software), and a new section 'Online Services Privacy & Security Terms' on its new Product Terms website.[79]

Even though the browser-applications and the mobile Office apps are not 'Core Online Services', Microsoft does provide (new) general and specific contractual guarantees about its role as data processor for both of these applications and services in Service Specific Terms.

[77] Microsoft Online Services Terms. The most recent available Word version from the OST dates from February 2021, URL: https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=18738 . Microsoft notes: "*Please note this is the last Online Services Terms Word document. Going forward, the terms will be published on the Product Terms site available at https://www.microsoft.com/licensing/terms/productoffering* "

[78] Microsoft Online Services Data Protection Addendum, 15 September 2021, URL: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

[79] Microsoft, Online Services Privacy & Security Terms, URL: https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EES

However, formal contractual roles are not decisive. A party's role must be determined based on the factual circumstances. In other words, it must be assessed who, in practice, determines the purposes and means of the processing.

5.3 Data processor

As a data processor, Microsoft may not determine what purposes are compatible with the main purpose of providing the service. The additional exclusions in the privacy amendment with the Dutch government that restrict usage for purposes such as profiling, data analytics, advertising and market research provide a clear demarcation against the use of Diagnostic Data as input for machine learning and artificial intelligence for 'you never know'.

The legal guarantees of the privacy amendment, and the updated information about Microsoft's role as data processor for the mobile Office apps and Office for the Web should allow the Dutch government organisations and universities to fulfil their role as data controllers for all Diagnostic Data relating to the use of Teams, OneDrive, SharePoint and the Azure AD, and to be in control over their compliance with data protection legislation. However, this DPIA shows that Microsoft does not yet fully apply these contractual guarantees correctly. Accidentally, Microsoft acted as a (joint) controller with regard to specific transfers of personal data to itself (Bing) as a controller, and by continuing to allow traffic to Cloudflare from Support pages.

5.4 Data controller

Pursuant to the privacy amendment with the Dutch government, Microsoft may only process limited, generally aggregated personal data for a limitative list of its own legitimate business purposes, where necessary.

As described in Sections 2.3.1, 2.3.2 and 2.3.3 Microsoft allows Teams on Windows to communicate personal data to third parties by default, sends personal data from SharePoint Online to itself in a role as data controller, and redirects Teams users to its support website from where it sends traffic to Cloudflare. This means Microsoft does not always factually behave as a processor.

The third parties accessed through the Teams store, Bing and Cloudflare are independent data controllers that may process the data for their own marketing purposes. Their processing operations are likely not limited to the three authorised processor purposes. Microsoft has made it possible, through the programming of the code, that these third parties receive personal data from Enterprise license end-users. In doing so, Microsoft has at least partially determined the purposes for this data processing. Admins can only opt-out from the first type of data processing, by disabling external applications in the Teams store interface for end users, but admins cannot block the other two types of data processing. Only a controller may determine the purposes of the processing. By enabling (not preventing) this processing, Microsoft is behaving as a (joint) data controller.

5.4.1 Controller Connected Experiences

As a result of the 2019 negotiations with the Dutch government, Microsoft has shifted its role for many of the most frequently used Connected Experiences, such as the Editor, to a role as data processor. Conversely, Microsoft is a data controller for the remaining Controller Connected Experiences. As described in Section 3.1.2 access to the Controller Connected Experiences was centrally blocked in the test tenant. However, this option was not effective on SharePoint Online: in the browser Microsoft

allowed traffic to be sent to Bing as part of the Controller Connected Experience Insert a picture. In reply to this DPIA Microsoft has committed to remove all such usage of Controller Connected Experiences in SharePoint when an organisation has disabled them.

5.4.2 *Disclosure to law enforcement and secret services*

Microsoft includes a list of specific purposes of data processing in its OST and DPA related to business operations for which Microsoft is a data controller. These purposes range from the obvious (sending invoices, creating statistics for the annual financial reports) to the often forgotten, such as complying with orders from law enforcement.

Through the amendment negotiated with the Dutch government and SURF in 2019, it is clarified that Microsoft does not act as a data processor when it has to hand over personal data (be it content, or Diagnostic Data) to a law enforcement authority, security agency or secret service in the USA, when Microsoft is not allowed to inform the customer and not allowed to redirect the order to the data controller. In those circumstances, Microsoft acts as a data controller, to comply with legal obligations imposed under US American law. Section 7 of this report describes the additional guarantees provided by Microsoft to minimise the chance that this situation occurs, in the initiatives 'We defend your data' and the development of the EU Data Boundary.

Based on the Schrems-II ruling, a recent expert legal analysis for the Dutch government, the analysis made by US law professor Stephen I. Vladeck (for the conference of the German State DPAs[80]), the report from Ian Brown and Douwe Korff for the LIBE committee of the European Parliament[81] and input provided to SLM Rijk and SURF by multiple cloud providers in 2021, an overview was created of US laws that may be applied to compel US cloud services providers to disclose personal data from EU Enterprise and Education customers.

Microsoft qualifies as electronic communications service provider as defined in Title 50 of the United States Code (USC) § 1881(b)(4). The definition is as follows.

> *The term "electronic communication service provider" means—*
>
> *a) a telecommunications carrier, as that term is defined in section 153 of title 47;*
>
> *b) a provider of electronic communication service, as that term is defined in section 2510 of title 18;*

[80] Prof. Stephen I. Vladeck, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, 15 November 2021, URL: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf. Professor Vladeck previously acted as expert (together with Peter Swire) on behalf of Facebook in the Schrems-II case at the European Court of Justice, where he defended US intelligence gathering as offering 'essentially equivalent' protections, similar to the essential data protection guarantees in the EU. See for a summary of his points, IAPP, Understanding 'Schrems 2.0', URL: https://iapp.org/news/a/understanding-schrems-2-0/ .

[81] Ian Brown and Douwe Korff, Study for the LIBE committee, Exchanges of Personal Data After the Schrems II Judgment, July 2021, URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

c) a provider of a remote computing service, as that term is defined in section 2711 of title 18;

d) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

e) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).[82]

This means Microsoft may be subjected to orders to hand-over personal data under FISA 702. Microsoft is legally prohibited from disclosing such orders.

This table assumes Microsoft also qualifies as "remote computing services" or "electronic communication services" (applicability of US Stored Communications Act and US CLOUD Act).[83] This table does not include legal obligations related to other US companies in other industries, such as banks or telecommunications carriers.

Table 4: Overview of US law that can be used to obtain personal data from EU Customers

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
Non-Disclosure orders can be issued up to one year[84] and have become 'commonplace'.[85] No principled restrictions on transparency reporting		Non-disclosure orders or general secrecy requirements. Transparency	

[82] See the official law website of the US government: https://uscode.house.gov/

[83] "Remote Computing Service[s]" ("RCS") and "Electronic Communication Service[s]" ("ECS") are defined in 18 U.S.C. § 2510(15): "'*electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications*"); and 18 U.S.C. § 2711(2) *("'remote computing service' means the provision to the public of computer storage and processing services by means of an electronic communications system*").

[84] A judge can issue a protective order for all SCA and CLOUD Act orders "*when the independent judge determines that there is reason to believe that notification of the existence of the court order may create the adverse result of (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.*" US Department of Justice, The purpose and impact of the CLOUD Act, Q&A 28, URL: https://www.justice.gov/dag/page/file/1153466/download The gagging orders are based on 18 U.S.C. § 2705. The maximum period of one year is mentioned in a memorandum from the Deputy Attorney General, 19 October 2017, URL: https://www.justice.gov/criminal-ccips/page/file/1005791/download.

[85] According to testimony of Microsoft VP Tom Burt for the House Committee on the Judiciary, 30 June 2021, URL: https://blogs.microsoft.com/on-the-issues/2021/06/30/the-need-for-legislative-reform-on-secrecy-orders/.

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
		reporting is only permitted in ranges.[86]	
US Stored Communications Act, also allows for preservation orders for specific records/evidence[87]	Content Data: warrant signed by a judge. Requires *probable cause*.	Executive Order of the President (E.O.) 12333 as amended (limited) by Presidential Policy Directive (PPD) 28.[88] Since January 2021 Specified in NSA SIGINT Annex[89]	Does not give direct authority to NSA to order cloud providers to hand-over data, but allows for bulk interception of transatlantic cables
	Non-Content Account Data (for example names and IP-addresses)[90] subpoena from court, prosecutor or agency (judge not required)		
	Other Non-Content (for example device information)[91]: court order or search warrant signed by a judge, lower standard of proof than for Content Data		

[86] The secrecy requirements are defined in 18 U.S.C. § 1874, but the USA Freedom Act of 2015 authorizes four different options for companies to publish numerical information about the NSLs and FISA orders they receive.

[87] Clause 2703(f) of the US Stored Communications Act.

[88] Presidential Policy Directive 28 does not authorize intelligence gathering. It imposes limitations on how signals intelligence is gathered through other authorized means when targeting non-U.S. persons (e.g., the why, whether, when and how the intelligence community targets foreign communications). Those means are articulated in the FISA 702 legal framework.

[89] NSA Sigint Annex, Procedures governing the conduct of DoD intelligence activities: Annex governing signals intelligence information and data collected pursuant to section 1.7(c) of E.O. 12333, URL: https://assets.documentcloud.org/documents/20454757/redacted-annex-dodm-524001-a.pdf

[90] The full list of 'Basic Subscriber Information' is defined in Title 18 of the United States Code (about Crimes and Criminal Procedure), U.S.C 2703(c)(2), *Required disclosure of customer communications or records*.

[91] 18 USC 2703(c)(1) and 18 U.S.C. 2703(d), Record[s] or other information pertaining to a subscriber to or customer of such service.

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
	Emergency requests: voluntary hand-over by providers (in case of imminent danger/death/serious physical injury)[92]		
US CLOUD Act (Clarifying Lawful Overseas Use of Data Act)	Expands the scope of the US Stored Communications Act to data stored outside of the EU, same authority requirements as above	Foreign Intelligence Surveillance Act (FISA) Section 702, limited to queries about non-U.S. persons located abroad. Section 702 no longer allows for the use of keywords. Sunset of FISA Section 702 by the end of 2023	Annual authorisation by the FISA Court (FISC).[93] FISC has authorized the collection of both metadata and content of communications
Electronic Communications Privacy Act (ECPA), created amendments on the Stored Communications Act and the Wiretap Act and created the Pen Register Act.	Information relating to subscribers of "*wire or electronic communication service providers*."[94] Signed by a judge or customer notice of such requests	National Security Letters (FBI) based on ECPA	No prior approval from a judge, when relevant to authorized national security investigations. Can only order access to Basic Subscriber Information, no

[92] 18 U.S.C. 2702(c)(4).

[93] According to the U.S. Department of Commerce most U.S. organizations do not handle data that U.S. intelligence agencies are interested in and therefore do not engage in data transfers that present the type of privacy risks that appear to concern the ECJ. The Annual Statistical Transparency Report for 2020, published by the Office of the Director National Intelligence identifies the following number of Section 702 court orders: 1 in 2018, 2 in 2019 and 1 in 2020, and notes the following estimated number of targets relating to such orders as 164,770 for 2018, 204,968 for 2019 and 2020723 for 2020. Published April 2021, URL: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2210-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2020.

[94] 18 U.S.C. 2709, et seq.

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
			content or diagnostic data.
Administrative subpoenas or demands (335 U.S. federal agencies)*	Based on the SCA, subject to the requirements described above	Title 1 (traditional) FISA warrant type a: existing account and metadata of U.S. Persons[95]	Applications to be approved by FISC
Search warrants to search and confiscate evidence, signed by judges based on state or local criminal laws (at least 57 distinct sets of laws[96])*	Based on the SCA, subject to the requirements described above	FISA warrant b: future metadata & content (tap) of U.S. Persons.	Applications to be approved by FISC
Judicially issued subpoenas and Grand Jury subpoenas for EU individuals to appear before a US court*	Based on the SCA, subject to the requirements described above	FISA business records order (Section 501, scope limited since 2020, no more 'any tangible thing'), for non-Content Data (Diagnostic Data)	Applications to be approved by FISC
Incoming Mutual Legal Assistance requests filed by EU law enforcement to US		FISA pen registers and trap and trace devices (as expanded by US Patriot ACT from	Applications to be approved by FISC, no

[95] US Congressional Research Service, Foreign Intelligence Surveillance Act (FISA): An Overview, 6 April 2021, URL: https://crsreports.congress.gov/product/pdf/IF/IF11451. *Applications for 'regular' FISA warrants must include the following: (1) the applicant's identity; (2) information regarding the target's identity if known; (3) why the target may be searched or surveilled; (4) a statement establishing a sufficient relationship between the target and the search location; (5) a description of what will be searched or surveilled; (6) a description of the nature of the information sought or of the foreign intelligence sought; (7) proposed minimization procedures; (8) a discussion of how the search or surveillance will be carried out; and (9) a discussion of prior applications. If electronic surveillance is sought, applications must also discuss the duration of the surveillance. Traditional FISA warrants are issued for US persons, but may lead to the incidental data collection of non-U.S. persons when the U.S. person is the target of the FISA collection because they are suspected to be "a foreign power" or "an agent of a foreign power."*

[96] As mentioned by Professor Vladeck in his expert paper for the German DPAs, p. 10.

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
Department of Justice Office of the International Affairs		2015 to internet communications)[97]	probable cause required

* Some of these law enforcement powers may not apply to data stored outside the United States, both in general and because of the strong presumption U.S. courts apply against the extraterritorial application of statutes.[98]

According to its semi-annual transparency report, in the first half of 2021, "*In the first half of 2021, Microsoft received 121 requests from law enforcement around the world for accounts associated with enterprise cloud customers. In 70 cases, these requests were rejected, withdrawn, no data, or law enforcement was successfully redirected to the customer. In 51 cases, Microsoft was compelled to provide responsive information: 31 of these cases required the disclosure of some customer content and in 20 of the cases we were compelled to disclose non-content information only. Of the 31 instances that required disclosure of content data, 27 of those requests were associated with US law enforcement.*"[99]

Microsoft explains that non-content data are Account and Diagnostic Data, "*such as an email address, name, state, country, ZIP code, and IP address at time of registration. Other non-content data may include IP connection history, an Xbox Gamertag, and credit card or other billing information.*"

Microsoft also explains that its statistics cover all orders, even if accompanied by non-disclosure orders. "*All government requests for data, including any that were accompanied by non-disclosure orders, also known as secrecy orders, are included in our transparency reports*."[100]

The number of requests for data from Enterprise customers is very low to the requests for consumer data. Microsoft writes: "*the overwhelming majority of requests seek information related to our free consumer services. By comparison, we have received*

[97] Applications do not require the identity of a suspect, only (1) the identity of the federal officer seeking to use a PR/TT device; (2) the applicant's certification that the information likely to be obtained is foreign intelligence information; and (3) a specific selection term to be used as the basis of the PR/TT device.

[98] As mentioned by Professor Vladeck, with a reference to Supreme Court jurisprudence from 2016, RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090, 2099–100 (2016).

[99] Microsoft, How many enterprise cloud customers are impacted by law enforcement requests? URL: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

[100] Idem, answer to the question 'Are legal demands subject to secrecy orders included in your reporting?'

very few requests for data associated with use of our commercial services used by enterprise customers."[101]

With regard to disclosures under the US Cloud Act, Microsoft writes it only complied once with such a request in the second half of 2020 relating to a non-US Enterprise customer, and with two such requests in the first half of 2021. These disclosed data do not necessarily have to be from a European customer: *"In the same time frame, Microsoft received 120 legal demands from law enforcement in the United States for commercial enterprise customers who purchased more than 50 seats. Of those demands, 2 warrants resulted in disclosure of content data related to a non-US enterprise customer whose data was stored outside of the United States."*[102]

Microsoft has announced in November 2021 it has never yet provided access to any personal data of public sector organisations in the EU to any government authority.[103]

5.5 Joint controllers

According to three judgments of the European Court of Justice[104] parties can factually become joint controllers, even if the roles are unevenly distributed, and also if the party that is the customer does not have access to the personal data processed by the party that supplies a service.[105]

Because the use of all different platforms for Teams, OneDrive and SharePoint is included in the Office 365 E3 or E5 license, government organisations and universities actually enable Microsoft to transfer personal data to itself as data controller, and to third parties.

As described above, Microsoft has committed to make improvements with regard to (unauthorised) traffic to third parties, such as Bing and has effectively enabled administrators to block traffic to Giphy and third-party apps in the Teams store.

With regard to the telemetry data, the administrators have no control at all over the events from Office for the Web. They cannot minimize the collection, they cannot inspect the data with a Data Viewer Tool or equivalent tool, Microsoft does not publish event-level information, and Microsoft does not provide access in response to a Diagnostic Data search, because most of the browser telemetry data are classified as *Required Service Data*.

---

[101] Microsoft blog, Q: What services are subject to law enforcement requests?, undated, https://blogs.microsoft.com/datalaw/our-practices/#does-microsoft-reject-us-subpoenas-from-government-seeking-content-data.

[102] Idem, answer to the question: *"Does Microsoft disclose additional data as a result of the CLOUD Act?"*

[103] Microsoft, Compliance with EU transfer requirements for personal data in the Microsoft cloud, November 2021, URL: https://go.microsoft.com/fwlink/p/?LinkID=2184913.

[104] European Court of Justice, C-40/17, 29 July 2019, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629, C210/16, 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein versus Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388. See in particular par. 38-43. Also see: C-25/17, 10 July 2018, Tietosuojavaltuutettu versus Jehovah's Witnesses — Religious Community, ECLI:EU:C:2018:551, par. 66-69.

[105] See for a more extensive explanation the umbrella-DPIA Office 365 ProPlus for SLM Rijk, 7 November 2018, p. 48-50.

Absent transparency about the browser telemetry and other *Required Service Data*, customers cannot instruct Microsoft to process these personal data on their behalf as a data processor. This in turn could lead to a factual qualification for some of this data processing as joint controllers. Microsoft's explanation that many *Required Service Data* are not personal data, needs to be verified. The data stream does not spontaneously flow to Microsoft, but originates from an end user device. A quick deletion of events or identifying data in an event may prevent data subject access, but cannot exempt Microsoft from its obligation as data processor to ask for instructions from its customer. To obtain such instructions, Microsoft must inform the customer in much more detail about the necessity of the collection of these data, and the necessary retention periods.

It follows from the technical analysis that Microsoft collects directly identifiable usernames in some events related to the use of OneDrive. This collection is in direct contradiction of Microsoft's promise never to process such directly identifiable data, or content data, in this undocumented category of telemetry events. In reply to this DPIA, Microsoft has explained that it will continue with this data collection, with many assurances. Microsoft has explained the exceptional necessity for this type of data collection, the separate data collection, short retention period and strict access governance rules. However, in order to prevent a factual qualification as joint controllers with the Enterprise and Education customers, these reassurances need to be independently verified, and Microsoft should be more transparent about this processing.

6. Interests in the data processing

This section outlines the different interests of Microsoft and the universities and government organisations. The interests of the government organisations and universities may align with the interests of their employees and students. However, this sector does not mention the fundamental data protection rights and interests of data subjects. How their rights relate to the interests of Microsoft and the public sector organisations is analysed in part B of this DPIA.

6.1 Interests of the government organisations and universities

The Dutch government organisations and universities have security, efficiency and compliance reasons to use Office 365 cloud services, such as Teams, SharePoint and OneDrive.

With Teams, users can directly and securely share information with each other and with a group of co-workers, instead of distributing it (as an attachment in the mail). Similarly, file sharing is easier and safer with OneDrive. Many organisations still share files via network drives for document storage or via local SharePoint servers. In practice, many employees and students share information via consumer versions of cloud products because existing solutions with network drives and SharePoint 2013 are not sufficient. Many people use, for example, Google Workspace, Dropbox, WeTransfer and Google Docs to share files. This can result in a parallel network that the government organisations and universities cannot manage.

It is a well-known ICT problem to properly organise and manage the authorisations for access to the network drives. If users have access to documentation to which they should not have access based on their role, this results in multiple security and privacy risks. In contrast to the network drives, the cloud storage services SharePoint and OneDrive offer transparency about the rights that have been granted for access to

the information. This also allows each end user to see who has access to which information. Additionally, the Azure AD enables admins to determine and enforce conditional access rules to personal data and information processed by the organisation. Use of the Azure AD also allows admins to take privacy-protecting measures by enabling Single Sign-On for interactions with independent software systems from third parties.

The government organisations and universities have strong efficiency reasons to move to the public cloud. A study of the 'cloudification' of universities in seven countries (the U.S., the U.K., Germany, Switzerland, Austria, the Netherlands, and France) and in the Times Higher Education (THE) Top 100 shows that the Dutch universities, together with UK, US and THE Top 100 universities have frequently migrated universities' core functions and services to public clouds, starting long before the COVID-19 pandemic.[106] The study describes several reasons for the uptake of public cloud services. For Teams, OneDrive and SharePoint the observation is useful that *outsourcing allows universities to not only reduce the needed local expertise to run these tools, but also allows the outsourcing of responsibility in case these tools become inoperable. Especially for highly business critical applications, as for example email or security management, cloud setups promise higher reliability."*[107]

The government organisations and universities have a strong general interest in providing reliable, always on, well integrated and location independent productivity tools to their employees. Well-functioning also means that the software has to be accessible on different kinds of devices, and from different locations. The ability for employees and students to seamlessly work at home and collaborate with each other through videoconferencing tools such as Teams, is as urgent as it was at the outbreak of the COVID-19 pandemic. Even if the pandemic subsides, it is plausible that many employees and students will continue to work more time at home than before 2021, and thus, are reliant on well-functioning online collaboration tools.

Additionally, the ability to access log data about user behaviour through audit logs in Office 365 is essential for government organisations to comply with their own obligations as data controllers to detect security incidents. Through the Content Search on the diagnostic log files, the Dutch government organisations' administrators can access data about users' access to personal data stored in OneDrive or SharePoint. This information is necessary in order to be able to detect possible security incidents and to be able to end security or data breaches.

6.2 Interests of Microsoft

Microsoft has explained its move to the cloud as necessary to drive up the security of services. Microsoft considers it a vital interest for society, as well as a business and economic interest, to be able to process large amounts of data in the cloud to be able to detect and defend against security threats. Local solutions are inevitably more expensive and probably less effective in detecting security incidents. Though Microsoft will offer its EU Enterprise and Education customers exclusive data processing in the EU at the end of 2022, this will not be the case for the security data. Microsoft writes:

[106] Tobias Fiebig, Seda Gürses, Carlos H. Gañán, Erna Kotkamp, Fernando Kuipers, Martina Lindorfer, Menghua Prisse, Taritha Sari, Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds, 19 April 2021. Available at URL: https://arxiv.org/abs/2104.09462. The study includes universities in Europe, UK and the US (and the Top 100).

[107] Idem, p. 3.

"*We must ensure that our European-based customers receive the same world-class security as our customers throughout the globe. Any data transfers outside the EU for security purposes will be limited in scope to what is needed for this purpose. This will allow us to provide the secure environment that our customers expect while meeting regulatory requirements by prohibiting unrelated secondary uses and implementing additional supplementary measures.*"[108]

Microsoft has clear business continuity interests in promoting its cloud ecosystem. Since 2014 Microsoft has as a mission to be cloud first and mobile first.[109] Microsoft explains: "*Our users don't simply use a workstation at a desk to do their jobs anymore. They're using their phone, their tablet, their laptop, and their desktop computer, if they have one. It's evolved into a devices ecosystem rather than a single productivity device (…).*"[110]

Microsoft has explained to SLM Rijk that it competes with other large-scale cloud providers and considers it an essential economic interest to be able to process large amounts of data to develop new services. "*But this* [the switch to Office 365 cloud-only service] *also brings enormous benefits. We already provide many intelligent services, combined with a service component. There is no question that we will analyse patterns and practices not only to improve security, but also to investigate whether there are new tools we want to build, also based on competitors, and questions from customers. This has to be possible. We will use data to the max, within what the law allows us.*"[111]

Microsoft has a strong financial and economic interest in selling customers a monthly cloud-based subscription service. For many years, Microsoft has been making a fundamental change in its business model: from a software products vendor to a monthly subscription service vendor. The vision of Microsoft is cloud-first, and pricing schemes strongly encourage the Dutch government and universities to switch from on-premise deployments to cloud only services. Microsoft is effectively putting pressure on institutions and universities to switch to the monthly model because it has ended its support for older versions, such as Office 2010.

Microsoft has also explained its economic (competition) interests and financial (monetisation) interests in the use of Diagnostic Data to show advice to the users of the software. Microsoft has explained that this type of advice was necessary in order to be able to compete with 'free' online products: "*These recommendations are necessary, because nobody goes on a course, we must integrate the manual in the software, because otherwise the users don't know what the features are. Our products take a direction to maximise use of products. That is what our customers expect*. *We help individuals to get the most out of their spending so that free products don't compete as well*. *Free products may have 80'% of our features, may be considered*

[108] Microsoft blog from Julie Brill, EU Data Boundary for the Microsoft Cloud: A progress report, 16 December 2021, URL: https://blogs.microsoft.com/eupolicy/2021/12/16/eu-data-boundary-for-the-microsoft-cloud-a-progress-report/

[109] Microsoft blog, Cloud-first, mobile-first: Microsoft moves to a fully wireless network, August 17, 2016, URL: https://azure.microsoft.com/nl-nl/blog/cloud-first-mobile-first-microsoft-moves-to-a-fully-wireless-network/.

[110] Idem.

[111] Microsoft Meeting report 30 August 2018, answer to Q46, quoted in the first public DPIA report on Office 2016 and Office 365 ProPlus.

good enough, but we need to distinguish ourselves with advanced productivity scenarios."[112]

Nonetheless, as a result of the ongoing negotiations with SLM Rijk and SURF, Microsoft has agreed to always act as a data processor for its online services, with a few exceptions. As a data processor, Microsoft is prohibited from using personal data from government organisations and universities in the Netherlands to show personalised recommendations for products or services of Microsoft the organisations have not purchased or do not use.

Microsoft also has an economic interest in certain default settings. Microsoft has claimed that it would suffer economic harm if the default setting for the use of Connected Experiences was default switched to "off".[113] Microsoft earned more than 8.53 billion dollars in the period from June 2019 to June 2020 with the sale of targeted advertisements in its search engine Bing.[114]

Finally, Microsoft has strong economic interests in mitigating the data protection risks for its EU customers. In May 2021, Microsoft's President Brad Smith announced that Microsoft is creating EU Data Boundaries, to allow organisations in the EU to exclusively process all data (from Core Online Services) in data centres in the EU.[115] This announcement marks a radical change of course for Microsoft. Microsoft does not offer a sovereign country cloud to countries, with the exception of the cloud for the federal USA government and the cloud for China. In 2019 Microsoft effectively terminated its national German cloud (no new customers accepted).[116] In the past few years, Microsoft declined to create an exclusive EU cloud for its EU Enterprise and Edu customers. This would involve high costs and be a barrier to innovation, according to Microsoft.[117] The change of course is due to the increasing concerns from EU customers about the legitimacy of the transfer of personal data to the USA. Microsoft plans to offer this new privacy option, called the EU Data Boundary, by the end of 2022. See Section 7 for more information about data transfers.

6.3 Joint interests

The interests of Microsoft and the Dutch public sector organisations align when it comes to the use of Diagnostic Data to protect the integrity, availability, and reliability of personal data in the online services. As part of the shared security interest, the provision of technical updates by Microsoft also concurs with the interests of the Dutch government organisations and universities, provided that the updates do not disrupt the service and that the technical administrators are able to disable or adjust the

[112] Idem, Meeting report 29 August 2018, answer to Q16.
[113] Idem, answer to. Q30.
[114] Statista, Microsoft Corporation search ad revenue 2016-2021, July 2021, URL: https://www.statista.com/statistics/725388/microsoft-corporation-ad-revenue/ .
[115] Microsoft blog Brad Smith, Answering Europe's Call: Storing and Processing EU Data in the EU, 6 May 2021, URL: https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/
[116] Microsoft (in German only), Microsoft stellt seine Cloud-Dienste ab 2019 aus neuen Rechenzentren in Deutschland bereit und reagiert damit auf veränderte Kundenanforderungen, 31 August 2018, URL: https://news.microsoft.com/de-de/microsoft-cloud-2019-rechenzentren-deutschland/ See also: Migration from Microsoft Cloud Germany (Microsoft Cloud Deutschland) to Office 365 services in the new German Data center regions. https://docs.microsoft.com/en-us/office365/enterprise/ms-cloud-germany-transition
[117] Meeting report 29 August 2018, answer to Q21.

updates.[118] Similarly, the interests are aligned that Microsoft needs to deliver a well-functioning (bug free) product, to facilitate working from home. Last but not least, Microsoft's announcement of EU data localisation for its EU Enterprise and Edu customers certainly aligns with the interest of government organisations and universities to use a public cloud service without sacrificing fundamental privacy rights.

In sum, Microsoft has financial, economic and commercial/business interests in the collection of Diagnostic Data and the ability to use it for all the purposes mentioned in this report. Some interests are consistent with the Dutch government's interests, but others are not.

7. Transfer of personal data outside of the EU

7.1 Microsoft's factual transfers of personal data to the USA

Until Microsoft has completed its EU Data Boundary, by the end of 2022, Microsoft systematically transfers some personal data from its EU customers to the USA.

Microsoft already enables its EU Enterprise and Edu customers to store some Content Data exclusively in the EU. This concerns a subset of Content Data of the Core Online Services, which Microsoft defines as *Customer Data*. Since these servers are located in the EU, the system-generated server logs about the individual use of these Core Services are also processed in the EU.

Additionally, Microsoft has changed the data processing for the Account Data in the Azure Active Directory (Azure AD). The content data are stored in the data centre where the Azure AD service is running, i.e., in the case of Dutch government organisations and universities, this means in data centres in the Netherlands and Ireland. "Azure Active Directory (Azure AD) stores customer data in a geographical location based on the address an organization provides when subscribing to a Microsoft online service such as Microsoft 365 or Azure."

Microsoft does not yet offer the possibility to administrators to exclusively process the Support Data and the Telemetry Data in the EU. Similarly, Telemetry Data and the system-generated log files about Online Services that are not Core Services also directly transferred or generated on Microsoft servers in the USA. Once the EU Data Boundary is in place, the Content Data and all related personal data from Microsoft 365, Dynamics 365, and Power Platform customers located in the EU or EFTA will automatically be included in this boundary. Customers no longer have to actively select this geolocalisation option.[119]

The logs created by the use of the Azure AD do not contain personal data such as usernames, phone numbers, or IP addresses. However, the UserObjectId identifies

[118] To the extent legally allowed without separate consent by the ePrivacy Directive and future ePrivacy Regulation. Roughly summarized and pending the resolution of political differences of opinion between the member states in the Council and the European Parliament, separate consent is and will not be necessary if the process is transparent, the update does not change the privacy settings, and does not change the types of personal data and purposes for which they are processed. Additionally, the user must be given an option to refuse the update.
[119] Microsoft reply to this DPIA report, 14 February 2022.

authentication attempts to users. These logs, and activity reports, are already stored in the customer region[120], as well as push notifications from Microsoft Authenticator app. The only exception is the use of voice calls with custom greetings for Multi Factor Authentication. Such calls are processed in an MFA backend in the United States.[121]

Contractually Microsoft only offers guarantees for the stored data (*data at rest*). The Customer Data can be routed via other locations during the transfer and can also be processed in other regions. Microsoft has explained that processing can take place at any location where Microsoft operates (except in China, as this is a completely separate cloud). This also applies to data replication. This is explained in section 10 of this report, 'Retention Periods'.

A comment needs to be made about the risks of undue access to the Content Data in transit. There is an innocent technical explanation why Microsoft does not provide legal guarantees about the data in transit. Microsoft encrypts all transit traffic anyway. Technically, the routing of packets via the Internet works in such a way that the paths (and therefore locations) that will be followed cannot be determined in advance. That is why there is no need for Microsoft to give legal confidentiality guarantees for the traffic in transit.

Microsoft describes the different data centres it uses for the different Office 365 services. It differs per service in which data centres the data at rest is stored. Content data from Teams, SharePoint and OneDrive from Dutch customers are stored in data centres in the Netherlands and Ireland.[122] Data processed for Viva Insights Advanced (including Workplace Analytics) are processed in the USA.

Following the DTIA completed for **the transfer of diagnostic personal data from Teams, OneDrive and SharePoint to the USA**, the risk of the transfer of these data can be assessed as low, primarily in view of the termination of these structural transfers in less than one year from now. However, even after completion of its EU Data Boundary for its core Online Services, Account Data and Support requests from EU customers, Microsoft will continue to incidentally transfer some personal diagnostic data to the USA for security purposes. Though Microsoft takes many steps to pseudonymise and aggregate these data about threats and malicious activities on customer' servers and end user devices prior to the transfer, Microsoft can still transfer pseudonymised personal data such as device identifiers and IP addresses to its centralised security monitoring and logs.

7.2 GDPR rules for transfers of personal data

The GDPR contains specific rules for the transfer of personal data to countries outside the European Economic Area (EEA). In principle, personal data may only be

[120] See the Azure AD data location map at https://msit.powerbi.com/view?r=eyJrIjoiYzEyZTc5OTgtNTdlZS00ZTVkLWExN2ItOTM0OWU4NjljOGVjIiwidCI6IjcyZjk4OGJmLTq2ZjEtNDFhZi05MWFiLTJkN2NkMDExZGI0NyIsImMiOjV9

[121] Microsoft, Data residency and customer data for Azure Multi-Factor Authentication, 12 January 2022, URL: https://docs.microsoft.com/nl-nl/azure/active-directory/authentication/concept-mfa-data-residency

[122] Microsoft, Where is your data located, 12 March 2021, URL: https://products.office.com/nl-NL/where-is-your-data-located?ms.officeurl=datamaps&geo=Europe#Europe See also: Where your Microsoft 365 customer data is stored, 3 December 2021, URL: https://docs.microsoft.com/en-gb/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide

transferred to countries outside the EEA if the country has an adequate level of protection. That level can be determined in a number of ways: a multinational may adopt Binding Corporate Rules, apply the EU Standard Contractual Clauses (SCC) or only transfer to countries for which the European Commission has taken a so-called adequacy decision.

7.1.1 Standard Contractual Clauses

Personal data may be transferred from the EEA to third countries outside of the EEA using Standard Contractual Clauses (SCC, also known as EU model clauses) adopted by the European Commission.[123] These clauses (hereinafter: SCC) contractually ensure a high level of protection.

7.1.2 European Commission Adequacy decision

An adequacy decision means that the country in question has a level of protection comparable to that applied within the EEA. Currently, there are adequacy decisions with respect to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the UK and Uruguay.[124] The adequacy decision for (some transfers under the Privacy Shield to) the USA is no longer valid since the summer of 2020.

7.1.3 Schrems-II ruling European Court of Justice: FISA Section 702 and E.O. 12333

On 16 July 2020, the European Court of Justice ruled that transfer of personal data based on the Privacy Shield was no longer valid, with immediate effect.[125] This judgment was the outcome of the lawsuit Max Schrems conducted against Facebook Ireland and the Irish Data Protection Commissioner. Earlier, in 2015, in another case instigated by Max Schrems, the European Court ruled the Safe Harbor agreement invalid, the predecessor of the Privacy Shield.

The Privacy Shield itself is since invalid as a legal basis for the transfer of personal data. The Court cited as the main reasons that the restrictions on privacy arising from the U.S. regulations are insufficiently defined and disproportionate and therefore constitute too great an invasion of privacy. Specifically, the Court describes the risks of mass surveillance (bulk data collection) by U.S. intelligence agencies under the surveillance programs PRISM and Upstream based on Section 702 FISA and based on E.O. 12333, and the lack of effective and enforceable rights for EU residents in the processing of those data by U.S. government agencies.

7.1.4 US Cloud Act and other applicable US law

In addition to these two specific surveillance powers, the USA legal regime enables law enforcement authorities and secret services to compel cloud providers to disclose personal data from their European customers, also when the data are stored in data

---

[123] Based on the Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/6794 June 2021, URL: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf

[124] European Commission, Adequacy decisions, URL last visited 28 January 2022: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[125] European Court of Justice, C-311/18, Data Protection Commissioner against Facebook Ireland Ltd and Maximillian Schrems (Schrems-II), 16 July 2020.

centres in the EU. Table 4 in Section 5.4.2 contains all known US laws that can be applied to Microsoft.

The US CLOUD Act (*Clarifying Lawful Overseas Use of Data*) was specifically designed to obtain access to data stored in data centres in the EU. This act extends the jurisdiction of North American courts to all data under the control of U.S. companies, even if those data are stored in data centres outside the territory of the United States.

As explained by the EDPB and the European Data Protection Supervisor (EDPS) in their opinion on the CLOUD Act to the LIBE Committee of the European Parliament, transfers of personal data from the EU must comply with the Articles 6 (lawfulness of processing) and 49 (derogations for specific situations) of the GDPR. In case of an order based on the US CLOUD Act, the disclosure and transfer can only be valid if recognised by an international agreement between the EU and the USA.

The EDPB and EDPS write: "*Unless a US CLOUD Act warrant is recognised or made enforceable on the basis of an international agreement, and therefore can be recognised as a legal obligation, as per Article 6(1)(c) GDPR, the lawfulness of such processing cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject on the basis of Article 6(1)(d) read in conjunction with Article 49(1)(f).*" [126]

In their cover letter, the data protection authorities emphasise "*the urgent need for a new generation of MLATs to be implemented, allowing for a much faster and secure processing of requests in practice. In order to provide a much better level of data protection, such updated MLATs should contain relevant and strong data protection safeguards such as, for example, guarantees based on the principles of proportionality and data minimisation.*" Additionally, the data protection authorities refer to the ongoing negotiations since 2019 about an international agreement between the EU and the US on cross-border access to electronic evidence for judicial cooperation in criminal matters and negotiating directives. [127]

Only the UK has so far signed a specific agreement with the USA for the Cloud Act. Negotiations between the EU and the US about updated MLATs, as well as negotiations about a successor for the Privacy Shield, did not produce any results yet. [128]

7.3 Data Transfer Impact Assessment (DTIA)

Microsoft uses the SCC to legitimise the transfer of personal (Diagnostic, Account and Support) data from its EU customers to the USA. According to the latest available

[126] Annex EDPB and EDPS joint response to US CLOUD Act, 10 July 2019, p. 8. URL: https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[127] Council Decision authorising the opening of negotiations, 6 June 2019, URL: https://data.consilium.europa.eu/doc/document/ST-10128-2019-INIT/en/pdf and https://data.consilium.europa.eu/doc/document/ST-10128-2019-ADD-1/en/pdf.

[128] See an update in US based news source Politico, Digital Bridge: Privacy Shield update 3.0 — Semiconductor subsidies — EU-US policy spat, 3 February 2022, URL: https://www.politico.eu/newsletter/digital-bridge/privacy-shield-update-3-0-semiconductor-subsidies-eu-us-policy-spat/

version of its Data Protection Addendum, Microsoft still uses the 2010 EU Standard Contractual Clauses, but it also commits to comply with the new 2021 SCC.[129]

Although the European Court of Justice recognizes the validity of the decision of the European Commission with which it adopted the SCC, and data transfers on the basis of the SCC are therefore still permitted in principle, this validity cannot be assumed for systematic transfers of personal data to the United States.

The fact is that transfers via the SCC also require that the recipient country provides an adequate level of data protection as defined in EU law. Article 46(1) of the General Data Protection Regulation (GDPR) explains that this means that data subjects must have adequate safeguards, enforceable rights and effective legal remedies at their disposal. Whether this is the case, according to the Court, must be determined by the data controllers and cloud providers themselves.

The Court writes: "*The assessment required for that purpose in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country. As regards the latter, the factors to be taken into consideration in the context of Article 46 of that regulation correspond to those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.*" [130]

The EDPB explains that there are four guarantees that make limitations to the data protection and privacy rights as recognised by the Charter justifiable.[131]

These four guarantees are:

1. Processing should be based on clear, precise, and accessible rules

2. Necessity and proportionality concerning the legitimate objectives pursued need to be demonstrated

3. An independent oversight mechanism should exist

[129] Microsoft Data Protection Addendum (English, last updated 15 September 2021). Microsoft writes: "*This Attachment 1 is in addition to Microsoft's execution of the 2021 Standard Contractual Clauses. In the case of any inconsistency between this Attachment 1 and the 2021 Standard Contractual Clauses, the inconsistency shall be resolved so as to provide an adequate level of data protection for the Customer Data, Professional Services Data, and Personal Data under applicable law.*" The European Commission has announced it will develop new SCCs for transfer to companies to whom the GDPR already applies based on Art. 3(1) or 3(2) of the GDPR. The legal debate about these new SCCs is outside the scope of this DPIA.
[130] European Court of Justice, C-311/18, Data Protection Commissioner against Facebook Ireland Ltd and Maximillian Schrems (Schrems-II), 16 July 2020, par 104.
[131] EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, Adopted on 10 November 2020, URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeaneessentialguaranteessurveillance_en.pdf

4. Effective remedies need to be available to the individual

These criteria are essential guarantees, the EDPB adds, but not sufficient by itself to determine whether the legal regime of the third country offers an essentially equivalent level of protection.

It follows from the Schrems II ruling that the current legal regime in the USA, in particular FISA legislation, does not meet these four criteria, for the following reasons:

1. FISA Section 702 and E.O. 12333 do not indicate limitations on the powers they confer to implement surveillance programmes for the purposes of foreign intelligence.

2. US laws permit public authorities to have access on a generalised basis to the content of electronic communications. This must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.

3. The scope of the supervisory role of the oversight mechanism by the US Ombudsman does not cover the individual surveillance measures. It is doubtful whether the US Ombudsman meets the other elements for independence defined by the European Court of Human Rights in its jurisprudence about surveillance measures, such as independence from the executive, being vested with sufficient powers and competence and whether its activities are open to public scrutiny.

4. Closely related to the third guarantee, data subjects from the EU whose data are transferred to the USA cannot bring legal action before an independent and impartial tribunal in order to have access to their personal data, or to obtain the rectification or erasure of such data.

7.3.1 Analysis of the chances that the risk of undue access occurs

As part of this DPIA, a DTIA was performed. Such a DTIA is necessary to assess whether the SCCs offer an essentially equivalent protection to the transferred data to Microsoft. The DTIA is attached in Excel. The analysis is based on the format created by the Swiss legal scholar David Rosenthal, with some additions.[132]

The definition of 'transfer' is not clear. The EDPB suggests that there is no transfer when a cloud provider can promise that all data are exclusively processed in the EU: "*Keep in mind that remote access from a third country (for example in support situations) and/or storage in a cloud situated outside the EEA offered by a service provider, is also considered to be a transfer. More specifically, if you are using an international cloud infrastructure you must assess if your data will be transferred to third countries and where, unless the cloud provider is established in the EEA and it*

[132] David Rosenthal, EU SCC Transfer Impact Assessment (TIA) Toolbox, with templates/samples for the various jurisdictions and a questionnaire for assessing foreign lawful access laws, published under free Creative Commons "Attribution-ShareAlike 4.0 International" (CC BY-SA 4.0) license, URL: https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx

clearly states in its contract that the data will not be processed at all in third countries."[133]

In a footnote in its guidance on supplementary measures in case of transfer, the EDPB suggests that any access from a third country counts as a transfer: "*Please note that remote access by an entity from a third country to data located in the EEA is also considered a transfer*."[134] This DPIA assumes that the term transfer includes (the possibility) of orders from US government authorities to disclose personal data for EU customers, hence the need for a Data Transfer Impact Assessment, even for the streaming Content Data in Teams and the stored data in OneDrive/Sharepoint, even though they are already processed and stored in the EU.

The EDPB describes different elements of the risk assessment in its guidance on *technical measures processors and controllers can take to mitigate the resulting high data protection risks*[135]

The assessment must include:

- The relevant laws
- The purposes for which the data are processed
- The categories of data transferred and their sensitiveness
- Whether the data will be stored in the third country or whether there is remote access to data stored within the EU/EEA
- Role of the parties (public/private, processor/controller)
- All actors, including subprocessors
- The format of the data
- Possibility of onward transfers[136]

The relevant laws are outlined in Table 4 in this report. The purposes for which the data are processed, are limited to 3 technically necessary purposes to provide the requested communications and storage functionality. Organisations may process all kinds of different categories of data in the three applications: ranging from public information to sensitive and special categories of data. The DTIA shows that the

[133] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with
the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, Par. 13, p. 11.
[134] Idem, footnote 23.
[135] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, URL: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
[136] Idem, p. 15.

outcome of the risk assessment in this case is most dependent on the categories of data, and the format of the data (encrypted/anonymised/pseudonymised).

The risk assessment takes the differences into account between (i) laws governing US law enforcement access to remotely stored data, (ii) surveillance laws aimed at foreigners, such as FISA Section 702, and (iii) 'regular' FISA warrants for metadata, wiretaps, pen registers and business records.

While FISA Section 702 orders can theoretically be challenged by non-US persons through civil actions under the Administrative Procedure Act, it is very unlikely that such individuals are informed that their data have been accessed. Without such a notice, individuals don't know, and cannot seek redress.

Additionally, the protection of the Fourth Amendment of the US Constitution, which prohibits "unreasonable searches and seizures" and requires that a warrant must be based upon "probable cause" extends only to US nationals and citizens of any nation residing within the US. According to the US Supreme Court, foreigners who have not previously developed significant voluntary connections with the US cannot invoke the Fourth Amendment.[137]

The EU Court's assessment of the U.S. security agencies' bulk searches in the Schrems-II ruling implies that providers such as Microsoft cannot guarantee an adequate level of protection because they cannot oppose FISA Section 702 orders or otherwise in all circumstances provide effective measures against the interference created by the law of the USA with the fundamental rights of persons whose data are transferred to the U.S.A.

EU individuals have more redress options against US law enforcement orders based on ECPA. ECPA protects 'persons', including foreign nationals, and recovering damages does not require proof of actual harm.

US CLOUD Act orders are somewhere in the middle. Different from national security orders and letters, providers are permitted to provide notice to their customers about CLOUD Act orders and 'regular' FISA warrants, unless the government has obtained a gagging order. CLOUD Act requests and gagging orders must be authorised by judges, but the redress possibilities for non-US persons are still wafer thin, as they will only be informed about orders for their data based on the US Cloud Act if the data are used in a criminal case.[138]

Absent a specific agreement with the EU or with individual EU countries, there is still a conflict of law absent an EU-US agreement on the access to personal data in criminal matters. Therefore, it is unlikely requests under the US CLOUD Act comply with the European essential data protection guarantees.

7.3.2 Mitigating measure: encryption

One of the most effective measures to mitigate the transfer risks is the application of effective encryption (See Section 8.1 of this report). The DTIA also assesses the risks

[137] Quote from the Ad-Hoc-EU-US Working Group on Data Protection, quoted by Ian Brown and Douwe Korff in their study about transfers for the LIBE committee of the EP.

[138] See ECJ, Schrems-II, par. 181 and 182. U.S. surveillance programs conducted under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and EO 12333 do not grant surveilled persons actionable rights before the courts against the US authorities / rights which are enforceable against the US authorities in the courts.

of the application of bulk interception of the traffic in transit from the EU to the USA, based on E.O. 12333 as mitigated by PPD-28. The chance that surveillance authorities will obtain legible personal data from Teams, SharePoint and OneDrive is calculated as zero when calculated over a two-year time period. This is due to the standard encryption of all data in transit, not only between the EU and the US, but also between Microsoft's data centres.

Though Microsoft does not yet offer E2EE for all Teams conversations, organisations can encrypt stored data in OneDrive and SharePoint with their own Customer Key (key accessible to Microsoft) or with Double Key Encryption (key not accessible to Microsoft). They can also use an additional layer of protection to prevent access by Microsoft employees (Customer Lockbox). The availability of encryption is especially relevant for very sensitive personal data. Since Microsoft Double Key Encryption can only be applied from an end user device, this option is not available for recordings of Teams calls, automatically generated in the organisation's OneDrive. This leads to the following conclusion in the DTIA:

- the use of Microsoft Teams to exchange special categories of data is not permitted, since organisations cannot apply E2EE to conversations and file sharing with multiple participants.

- Recordings and transcriptions of Microsoft Teams conversations that may include sensitive or special categories of data are similarly not permitted.

- The storage of very sensitive and special categories of personal data in OneDrive or SharePoint is only permitted when the organisation has control over the key, with for example Double Key Encryption. Even a very small chance that the data can be unlawfully accessed by US law enforcement agencies or secret services, is not acceptable in that case.

- Conversely if organisations only want to share or store public data, they can use Teams and storage of data in the Microsoft cloud because even if the very small chance of undue access to these personal data occurs, it will have a low impact on the data subjects.

The DTIA does include the small risk that US surveillance authorities are so interested in a particular individual, that there is a 5% chance that the encrypted personal data are the subject of intelligence searches. It is plausible that some content data exchanged via Teams or stored in OneDrive and SharePoint by an EU gov or university organisation are considered interesting for intelligence searches, especially since Teams does not offer E2EE encryption for all calls yet, and not all stored data will be encrypted with Double Key Encryption. The DTIA does not calculate the risk of the decryption capacities in 10 or 20 years from now, or the likelihood of the assumption that the NSA is storing all intercepted metadata for future decryption purposes, as these assumptions are impossible to test or quantify.

7.3.3 Mitigating measure: transparency

Another important mitigating measure is if the transparency reports from the provider show that the practical chance of occurrence of this risk is almost zero, even though a low number of requests by itself cannot be used to assess the risk for data subjects as low.

The EDPB writes: "*you may decide to proceed with the transfer without being required to implement supplementary measures, if you consider that you have no reason to believe that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer. You will need to have demonstrated and documented through your assessment, where appropriate in collaboration with the importer, that the law is not interpreted and/or applied in practice so as to cover your transferred data and importer, also taking into account the experience of other actors operating within the same sector and/or related to similar transferred personal data and the additional sources of information described further below that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer.*"[139]

As explained in Section 5.4.2 Microsoft twice per year publishes a detailed transparency report about the amount of law enforcement requests and surveillance orders it has received. The number of requests for data from its Enterprise customers is very low. Microsoft has published in November 2021 that it has never disclosed personal data from any EU public sector customer to any government.[140]

Even though Microsoft has publicly raised alarm about the increasing amount of gagging orders , in practice, this risk apparently has not materialised for the Dutch government and universities. Microsoft clearly explains that it will disclose the number of orders received, regardless of a gagging order.

Competitors for Enterprise cloud storage and communication services such as IBM, AWS, Zoom, Cisco and Google have also published information about the number of requests they have received.

Google, like Microsoft, distinguishes between consumer and Enterprise accounts.[141] Though Google has received 185 requests in total in the second half of 2020, this does not mean Google has provided data in all of these cases. More importantly, Google does not explain where these Enterprise customers are located.

[139] EDPB Recommendations on supplementary measures, par 43, p. 18.

[140] Microsoft, Compliance with EU transfer requirements for personal data in the Microsoft cloud, November 2021, URL: https://go.microsoft.com/fwlink/p/?LinkID=2184913 .

[141] Google Transparency Report, Enterprise cloud requests for customer information, URL: https://transparencyreport.google.com/user-data/enterprise?hl=en_GB

Figure 27: Google statistics US law enforcement requests for global Enterprise customers

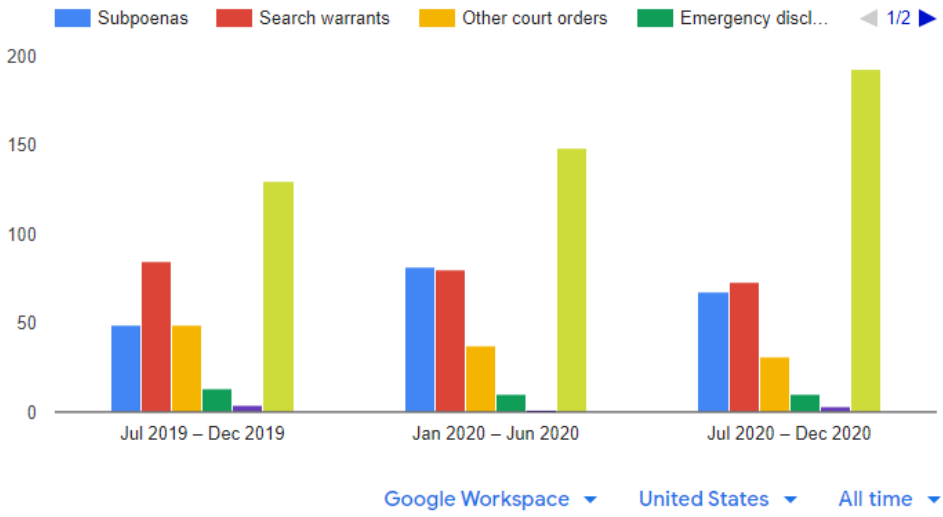
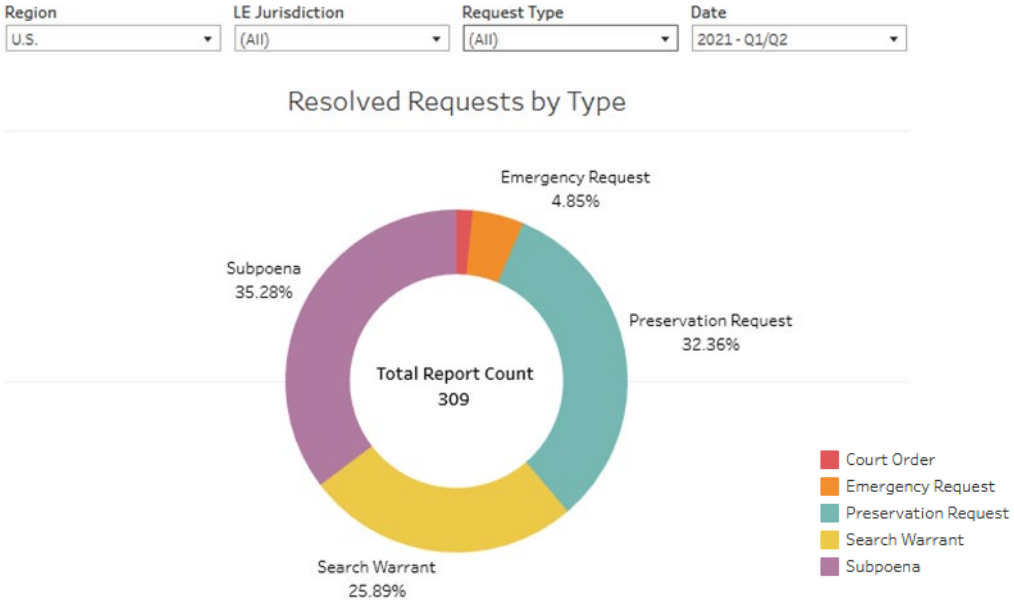


Figure 28: Zoom overview of US requests for all of its customers, January – June 2021[142]

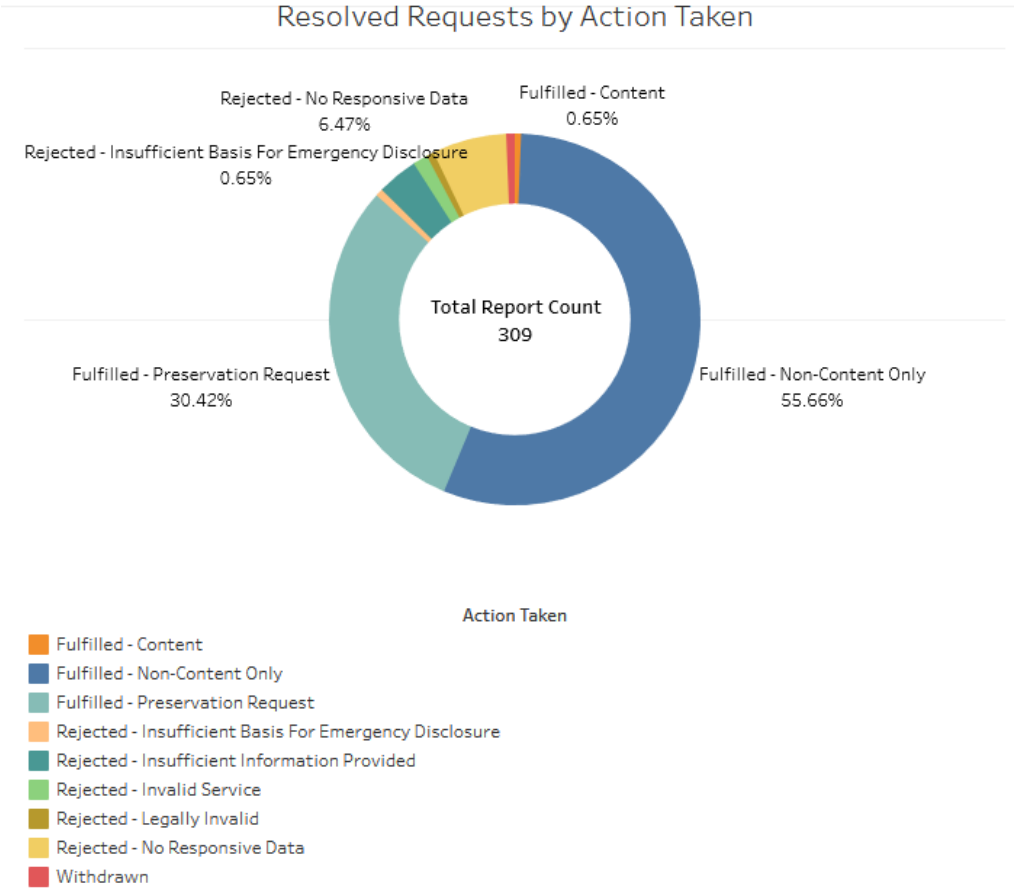


Zoom also publishes a bi-annual transparency report. Zoom does not distinguish between consumer accounts and Education/Enterprise accounts. Zoom received 309 requests from US law enforcement authorities in the first half of 2021 for all of its global customers. As Zoom does not mention any US Cloud Act, FISA 702 or National

[142] Idem.

Security Letters at all, the number of requests for personal data based on these powers is assumed to be zero. [143]

Figure 29: Zoom statistics about resolution of US requests, May – December 2020[144]



Videoconferencing ccompetitor Cisco also publishes bi-annual transparency reports.[145] Similar to Microsoft's and Google's reporting, Cisco also provides many different services, not limited to online communication services. In the first half of 2021, Cisco disclosed non-content data in 7 cases on demands from US law enforcement. For US national security demands. Cisco only reports in ranges, similar to Microsoft and Google, between 0 and 249 cases.

[143] Zoom second transparency report, URL: https://explore.zoom.us/docs/en-us/trust/transparency.html
[144] Idem.
[145] Cisco Transparency Report Jan-June 2021, URL: https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=transparency#/1640125994492149

Figure 30: Cisco statistics US law enforcement requests for global Enterprise customers

Reporting Period: January 1st -June 30st, 2021

Government Data Demands – United States (exclusive of National Security Demands, which are reported below)

Data Type Demanded	Total Demands	No Data Found	Total Rejected	Total Disclosed
Content Data	5	4	1	0
Non-Content Data	25	13	5	7
Emergencies	0	0	0	0

United States National Security Demands

Cisco may receive demands for data from U.S. national security organizations. These include Foreign Intelligence Surveillance Act (FISA) warrants, orders, directives, or National Security Letters (NSLs). The table below lists the number of U.S. National Security demands Cisco has received during the applicable period, subject to the limitations prescribed by the USA Freedom Act of 2015.

January 1st -June 30st, 2021	Totals
National security orders, directives, or national security letters received	0-249
Number of accounts affected under all national security orders, directives, or national security letters	0-249

In response to the decision from the Austrian DPA that a website could no longer use Google Analytics, because of the transfer of (pseudonymised) data to Google's servers in the USA, Google wrote: "*But Google has offered Analytics-related services to global businesses for more than 15 years and in all that time has never once received the type of demand the DPA speculated about. And we don't expect to receive one because such a demand would be unlikely to fall within the narrow scope of the relevant law.*"[146]

Another US business to business company, IBM, has for example explained that it has only received 1 CLOUD Act request, and refused to comply. The company has never provided client data stored outside of the US to the US government under any national security order, including FISA warrants.[147]

AWS provides the clearest assurance about the disclosure of Enterprise Content Data located outside the United States, namely: zero.[148] However, AWS did receive a total of 393 requests from US law enforcement in that period. AWS does not explain how

[146] Google in Europe, It's time for a new EU-US data transfer framework, 19 January 2022, URL: https://blog.google/around-the-globe/google-europe/its-time-for-a-new-eu-us-data-transfer-framework/

[147] Computer Weekly, IBM pushes back against US government data requests, 7 June 2021, URL: https://www.computerweekly.com/news/252501996/IBM-pushes-back-against-US-government-data-requests

[148] AWS Information Requests Report June-December 2021, published 31 January 2022, URL: https://d1.awsstatic.com/Information_Request_Report_December_2021_bia.pdf

many of these requests related to Non-Content data from customers in the EU. AWS also reports a range of 0-249 national security requests.

Figure 31: AWS answer to question about access to Content Data outside the US

How many requests resulted in the disclosure to the U.S. government of enterprise content data located outside the United States?
None.

Published January 31, 2022

In sum, based on Microsofts transparency reporting, and a comparison with other US companies offering more or less comparable services, the estimated number of 0.5 cases from US law enforcement and security orders combined per year for personal data from Microsofts public sector customers in the EU seems plausible.

7.3.4 *Mitigating measure: pseudonymisation and aggregation*

Even if the content data are encrypted with keys controlled exclusively by the customer, the Diagnostic, Account and Support Data cannot be encrypted, only protected with transport encryption. As described in Section 7.1, the Account Data and the service generated server logs for Teams, OneDrive and SharePoint are already exclusively processed in the EU. The service generated server logs contain all kinds of identifiable data and contents such as subject and file names. Microsoft can be compelled to provide access to these data stored in the EU, but the likelihood is near zero based on historical experience.
The Telemetry Data on the other hand are collected in a pseudonymised format. The in-built client in the end user applications and browser can be set to the level 'neither', and in that case, should not send any directly identifiable or content data to Microsoft in the USA. The only exception to this rule, as described in Section 2.2.1, is the inclusion of readable usernames in path names in OneDrive telemetry events. As this is exceptional, and Microsoft has vowed to minimise access authorisations, limit the storage of these events to max. 30 days, this risk can be accepted in combination with additional measures to protect employees whose identity must remain confidential, through the use of pseudonymous accounts.

7.3.5 *Other mitigating measures: privacy pledges and EU Data Boundaries*

Microsoft has a proven track record of legally objecting against orders for EU residents' data. In fact, a famous court case known as the Microsoft warrant case, which Microsoft won, was the origin of the US CLOUD Act in 2018, to legitimise such orders for personal data hosted in the EU.[149]

In November 2020, Microsoft launched new privacy commitments with regard to law enforcement orders for its EU Enterprise customers' data. The new program is called 'Defending your data' and is contractually guaranteed through a new addendum to the OST.[150] In the launching blogpost, Microsoft promises to take the following steps:

- *"First, we are committing that **we will challenge every government request for public sector or enterprise customer data** – from any*

[149] Microsoft blog, The CLOUD Act is an important step forward, but now more steps need to follow, 3 April 2018, URL: https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/
[150] Microsoft, We defend your data , URL: https://www.microsoft.com/en-ww/trust-center/privacy. The *Additional Safeguards Addendum to Standard Contractual Clauses* are available at https://aka.ms/defendingyourdataterms.

government – where there is a lawful basis for doing so. This strong commitment goes beyond the proposed recommendations of the EDPB.

- *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 General Data Protection Regulation (GDPR). This commitment also exceeds the EDPB's recommendations. It shows Microsoft is confident that we will protect our public sector and enterprise customers' data and not expose it to inappropriate disclosure."* [151]

Microsoft continues to resist secrecy through so-called *gagging orders*. In a blogpost from January 2021, Microsoft explains that it has received three such orders in 2020 and how it fights these orders.[152] In a blogpost from June 2021, Microsoft publishes the testimony from its Corporate Vice President Tom Burt for the House Committee on the Judiciary about the need for legislative reform to curb the secrecy orders.[153] In this post he raises public alarm about the increasing amount of *gagging orders*. Burt writes: *"Secrecy orders under 18 U.S.C. § 2705(b) – also known as non-disclosure orders – have unfortunately become commonplace. They are often approved even for routine investigations without any meaningful analysis of either the need for secrecy or the orders' compliance with fundamental constitutional rights."*[154]

Additionally, in May 2021, Microsoft committed to build a European cloud for its European Enterprise and Education customers before the end of 2022, as described in Section 6.2 of this report. If and when Microsoft indeed exclusively processes all personal data within the territorial boundaries of the EU, while it continues to apply effective transit encryption, also between its EU data centres, the risk of mass surveillance by the US security services would become much less likely. Of course, US authorities could still order access to personal data from individuals hosted in the EU, but the chance that Microsoft will disclose such data can be assessed as highly unlikely. Microsoft makes important pledges to fight each such request and compensate individual end-users in the EU if it were forced to hand-over their personal data. These commitments greatly raise the barrier for such requests to be filed.

7.3.6 Future developments: EDPS investigation and coordinated EDPB cloud investigation

On 27 May 2021 the EDPS announced it would start an investigation to verify compliance with its Recommendations[155] on the use of Microsoft Office 365 as contracted by the European Commission, and into the legitimacy of data transfers by

[151] Microsoft blog, Julie Brill, New steps to defend your data, 19 November 2020, URL: https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/

[152] Microsoft blog, Continued progress and support in fighting secrecy orders, 5 January 2021, URL: https://blogs.microsoft.com/on-the-issues/2021/01/05/secrecy-orders-protection-enterprise-data/.

[153] Microsoft blog Tom Burt, The need for legislative reform on secrecy orders, 30 June 2021, URL: https://blogs.microsoft.com/on-the-issues/2021/06/30/the-need-for-legislative-reform-on-secrecy-orders/

[154] Idem.

[155] EDPS, Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services, 2 July 2020, URL: https://edps.europa.eu/data-protection/our-work/publications/investigations/outcome-own-initiative-investigation-eu_en

public cloud infrastructure services offered by Microsoft (Azure) and Amazon (Amazon Web Services).[156]

The EDPS explains: "*These investigations are part of the EDPS' strategy for EU institutions to comply with the "Schrems II" Judgement so that ongoing and future international transfers are carried out according to EU data protection law.*"[157] No results have yet been published.

On 18 October 2021 the EDPB announced its first coordination on the use of Cloud based services by the public sector. The EDPB explains: "*In a coordinated action, the EDPB prioritizes a certain topic for supervisory authorities to work on at the national level. The results of these national actions are then bundled and analysed, generating deeper insight into the topic and allowing for targeted follow-up on both the national and the EU level the joint task force.*"[158] The head of this taskforce, Gwendal le Grand, wrote: "*In the first quarter of 2022, we will announce further details on the first topic that was chosen for coordinated action within the CEF, namely the use of cloud services by the public sector. The EDPB prioritised this topic because the increasing deployment of cloud services in the public sector triggers a number of data protection risks which require careful assessment.*"[159]

The outcomes of this DPIA have to be reassessed if the EDPS and/or the EDPB taskforce come to a different conclusion with regard to the high and low risks, especially regarding the ongoing (limited) data transfer to the USA and the mitigating measures described above.

8. Techniques and methods of the data processing

As explained in section 2 of this report, Microsoft collects personal data about the use of Teams and the cloud storage services in different ways. These are all Diagnostic Data according to the definition used in this report (see Section 1.3). One of the ways Microsoft collects Diagnostic Data is described below: through the Azure AD usage and multi factor authentication log files.

8.1 Encryption

Organisations can use Microsoft Double Key Encryption to prevent any (forced) access by Microsoft to the decrypted contents of their stored files in OneDrive or SharePoint.[160]

---

[156] EDPS press release, The EDPS opens two investigations following the "Schrems II" Judgement, 27 May 2021, URL: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en

[157] Idem.

[158] EDPB, EDPB launches first coordinated action, 18 October 2021, URL: https://edpb.europa.eu/news/news/2021/edpb-launches-first-coordinated-action_en

[159] EDPB, EDPB Support Pool of Experts: enhancing cooperation by complementing the strengths of SAs, 11 January 2022, URL: https://www.linkedin.com/pulse/edpb-support-pool-experts-enhancing-cooperation-complementing-/?trackingId=I0uTq7jPQHW6c1qQ%2FGJSzA%3D%3D

[160] See the report (in Dutch only) Privacy Company wrote for the Netherlands National Communications Security Agency (NBV), part of the General Intelligence and Security Service, about Double Key Encryption, 13 January 2021, URL: https://slmmicrosoftrijk.nl/wp-content/uploads/2021/02/Analyse-Microsoft-DKE-13-jan-2021.pdf

Microsoft does not yet offer end-to-end encryption for the streaming communication with multiple participants in Teams; only for unscheduled one-to-one video calls.[161] Though Microsoft's encryption of the conversations and exchanged files ensures protection against unauthorised access, incidental forced access to the content data by US authorities cannot be excluded. This means there is a high transfer risk for sensitive, confidential and special categories of personal data exchanged in regular Teams calls without end-to-end encryption, if such personal data are not publicly available, because the customer is not in control of the encryption keys.

Microsoft offers two relevant protection and encryption services for less sensitive personal data (in E5 licenses): Customer Lockbox and Customer Key.

- Customer Lockbox is a feature that helps to explicitly regulate access to document contents by Microsoft support engineers in Office 365. Access can be authorised by the customer for limited time frames and for specific purposes.[162]

- Customer Key is a feature for Office 365 that allows customers to control encryption keys for the encryption of data at rest. Microsoft still has access to the key when processing data. This feature reduces the opportunities Microsoft has to access customer data, but does not eliminate them.[163]

8.2 Big Data Processing

Until May 2019, Microsoft did not publish extensive documentation about the contents of diagnostic events it collects through the use of Office 365, including the cloud communication and storage services. Microsoft previously explained to SLM Rijk that prior to 2018 there were no central rules governing the collection of Diagnostic Data.[164] Since 2018 such rules are in place for new data, according to Microsoft.[165]

Microsoft has steadily increased its transparency about the Diagnostic Data it collects, with the exception of the telemetry events it collects from the browser-accessible versions of Teams, OneDrive and SharePoint, and with the exception of the category of *Required Service Data*.

Microsoft stores the Telemetry Data from Office 365 and Windows together with the Diagnostic Data from its cloud services in one central long-term database called Cosmos. A former Microsoft engineer gave a presentation on the architecture of Cosmos. He explains that Cosmos not only contains this Diagnostic Data, but also data from Skype, Xbox, Bing, Advertisements and more.[166] The engineer explains:

---

[161] Sinds 14 December 2021 voor de hele wereld, zie: https://techcommunity.microsoft.com/t5/microsoft-teams-blog/end-to-end-encryption-for-one-to-one-microsoft-teams-calls-now/ba-p/3037697

[162] Microsoft, Introduction to Customer Lockbox, URL: https://docs.microsoft.com/en-us/learn/modules/m365-compliance-insider-manage-customer-lockbox/introduction

[163] Microsoft, Set up Customer Key, 10 June 2021, URL: https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-key-set-up?view=o365-worldwide

[164] Meeting report 28 August 2018, answer to Q1.

[165] Microsoft confidential response to the first public Office 365 ProPlus DPIA report, 24 September 2018, p. 10.

[166] Presentation Eric Boutin. Meetup 5 November 2015, URL: https://www.slideshare.net/MemSQL/how-microsoft-built-and-scaled-cosmos (URL last visited on 15 March 2020, recorded on 12 July 2019)

"*Teams put their data in Cosmos because that is where the data they want to join against is.*" He also states that in 2015 there was a cluster of more than 50,000 servers.[167]

In an earlier presentation about Cosmos in 2011, two former Microsoft engineers explain: "*We ingest or generate a couple of PiB every day*

- *Bing, MSN, Hotmail, Client telemetry*
- *Web crawl snapshots*
- *Structured data feeds*
- *Longtail of other data sets of interest"*[168]

The existence of Cosmos has been confirmed by the auditors of EY at the request of SLM Rijk, in their *Assurance report on profiling restrictions with regard to Microsoft's Office 365 ProPlus*.[169] EY writes:

- "*EUPI data is stored in an internal data store called Cosmos, where data is stored in virtual clusters.*

- *access to virtual clusters in Cosmos is only possible through the use of a privileged access identity (separate Azure Active Directory)*

- *only qualified employees can request a privileged access identity and gain access to virtual clusters in Cosmos. When logged on to Cosmos with their Microsoft identity, users can view the Cosmos catalog but not enter any virtual clusters*."[170]

As cited in Section 4.3 of this report, Microsoft, as a controller/supplier of consumer services such as Bing, contractually allows itself to analyse data from various sources to predict interests and to send users 'relevant offers', as well as targeted advertisements, both in Microsoft products and services and on third-party websites.

Microsoft can continuously collect new types of Diagnostic Data, both on its own cloud servers and through the telemetry clients built into the Teams, OneDrive and Sharepoint applications on the different platforms (where available). Therefore, any analysis of the Diagnostic Data remains a snapshot. Data processing remains dynamic.

9. Additional legal obligations: e-Privacy Directive

This section only describes the additional obligations arising from the current ePrivacy Directive and (possible) future e-Privacy Regulation. In view of the limited scope of this DPIA, other legal obligations or frameworks (for example in the area of information security, such as BIO) are not included in this report.

---

[167] Ibid, slides 8 and 13.

[168] Pat Helland and Ed Harris, Cosmos, Big Data and Big Challenges, 26 October 2011, URL: http://web.stanford.edu/class/ee380/Abstracts/111026a-Helland-COSMOS.pdf (URL last visited 15 March 2020 and recorded 12 July 2019).

[169] SLM Rijk, EY Assurance Report on profiling restrictions with regard to Microsoft's Office 365 ProPlus, research conducted from 1 July 2020 to 30 September 2020, URL: https://slmmicrosoftrijk.nl/?smd_process_download=1&download_id=3053

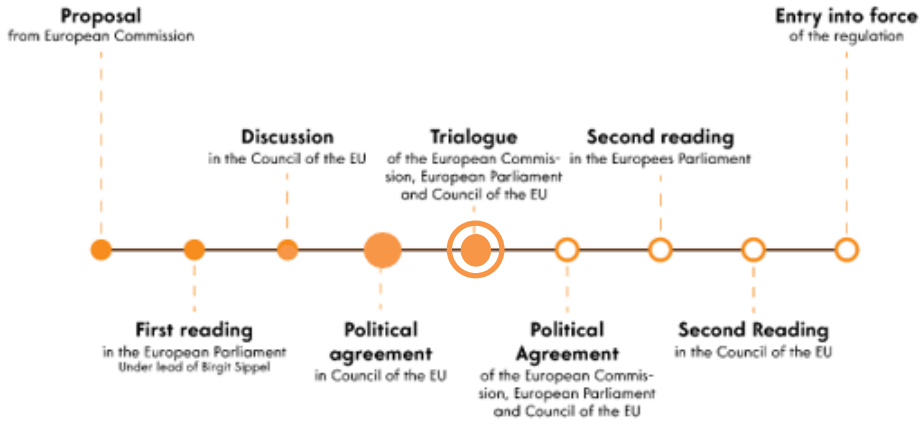
[170] Idem.

The only relevant change compared to the DPIA published 30 June 2020[171], is that the scope of the confidentiality requirements in the ePrivacy Directive has been extended to all electronic communications providers, including Teams.

The current ePrivacy Directive also includes rules on the confidentiality of data from the content and on communication behaviour. Article 5(1) obliges Member States to guarantee the confidentiality of communications and related traffic data via public communications networks and publicly available electronic communications services. Article 6(1) obliges providers of publicly available telecommunications services to erase or make the traffic data anonymous as soon as they are no longer needed for the purpose of the transmission of the communication.

Although the confidentiality rules in the ePrivacy Directive originally only covered classic telephony and internet providers, the scope was expanded significantly last year. Since the European Electronic Communications Code (EECC) became applicable law (21 December 2020)[172], the confidentiality rules apply to all *over-the top* communications services, such as Teams (and Microsoft's e-mail services) and other internet-based videoconferencing services.

Figure 32: Timeline new ePrivacy Regulation



The consent requirement for tracking cookies will likely continue to exist in the future ePrivacy Regulation. On 10 January 2017, the European Commission published a proposal for a new ePrivacy Regulation.[173] This was followed by an intense political debate the last four years. The European Parliament responded quickly and positively,

[171] DPIA on Microsoft Office 365 for the Web and mobile Office apps, published 30 June 2020, URL: https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps .

[172] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, L 321/36, 17 December 2018, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN.

[173] European Commission, Proposal for a Regulation on Privacy and Electronic Communications, 10.1.2017 COM(2017) 10 final, URL: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

but it has taken the representatives of the EU Member States three years to draft a compromise about the proposed ePrivacy Regulation. The Council sent its agreed position to COREPER to start the trialogue on 10 February 2021.[174] The most recent update from the Council dates from 12 November 2021.[175] In the first half of 2022, France has announced ePrivacy will be a priority during its Presidency of the Council.[176] However, the points of view of the European Parliament and the European Council are widely diverging. Therefore, it is not likely that the ePrivacy Regulation will enter into force anytime soon, and Microsoft will have to comply with the current ePrivacy and EECC rules in the next few years.

10. Retention periods

In the Data Protection Addendum belonging to the OST Microsoft has included one section on retention periods.[177] This shows that Microsoft retains Customer Data for 90 days after termination of the subscription, and actually deletes Customer Data and personal data after another 90 days.

"*Data Retention and Deletion*
At all times during the term of Customer's subscription, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service. Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data within an additional 90 days, unless Microsoft is permitted or required by applicable law, or authorised under this DPA, to retain such data.
The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data or Personal Data as described in this section."

In the privacy amendment with SLM Rijk and SURF, it has been agreed that Microsoft will not store personal Diagnostic Data for longer than 18 months after the initial collection.

Since May 2019, Microsoft has published somewhat more information about the various retention periods for Personal Data in Office 365.[178]

---

[174] Council of the European Union, Interinstitutional File 2017/0003(COD), Brussels, 10 February 2021 (OR. en) 6087/21, URL: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.
[175] Council of the European Union, Interinstitutional File 2017/0003(COD), Brussels, 12 November 2021, request for an amended mandate, largely blacked out, URL: https://data.consilium.europa.eu/doc/document/ST-13558-2021-INIT/en/pdf
[176] French Presidency of the Council of the European Union, Programme of the Presidency, URL: https://presidence-francaise.consilium.europa.eu/en/programme/programme-of-the-presidency/
[177] Microsoft Online Services Data Protection Addendum, 15 September 2021, URL: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA .
[178] Microsoft, Data Retention, Deletion, and Destruction in Office 365, 27 November 2021, URL: https://docs.microsoft.com/en-gb/office365/securitycompliance/office-365-data-retention-deletion-and-destruction-overview

Microsoft distinguishes between Customer Content (all text, sound, video, images and software created and stored in Microsoft data centres via Office 365 services), other Customer Data and Personal Data that are not part of Customer Data.

Table 5: Microsoft overview of data types and retention periods

Type of data	**Retention period**
Customer Content	30 days after the administrator has actively deleted the data, or passively by Microsoft, 180 days after the termination of the subscription
Content of chats in Teams	Six months, can be changed by admin[179]
Directly identifiable personal data, as user and/or screenname, IP-address	180 days
Other pseudonymous personal data	30 to 180 days. Microsoft deletes the directly identifiable data in OneDrive events within 30 days.
Azure AD multifactor authentication doesn't log personal data such as usernames, phone numbers, or IP addresses. However, UserObjectId identifies authentication attempts to users.	Log data are stored 30 days.[180] This includes Audit logs, sign-ins, Azure AD MFA usage and risky users/risky sign-ins.[181]

The table describes how long Microsoft retains data after a customer actively deletes the data, or after a customer terminates the subscription (passive deletion by Microsoft). This table is far from complete. Microsoft only describes unique identifiers in this table, but Microsoft omits to explain that it records and stores the individual actions of users in combination with the named identifiers.

[179] Microsoft, Teams Help, What's new in Microsoft Teams, 13 December 2019, URL: https://teams.microsoft.com/#/apps/5a0e35f9-d3c8-45b6-9dd9-983ab47f1b83/sections/release-notes?intent=1&category=16&autoNavigationOnDone=true&skipInstalledSuccess=false&preselectTeam=19:267e2fc2585c4cf1bf50a7bb969e444b@thread.skype&addAppDialogEntryPoint=20 *"Chat history increased Now, when you go on vacation, leave of absence, or simply need to send a message to that group discussion from last month, you'll find your chats right where you left them. Currently, chat history will remain in your chat list for up to six months."*

[180] Microsoft, Personal data stored by Azure AD multifactor authentication, 12 January 2022, URL: https://docs.microsoft.com/en-gb/azure/active-directory/authentication/concept-mfa-data-residency#personal-data-stored-by-azure-ad-multifactor-authentication .See

[181] Microsoft, How long does Azure AD store the data? 11 August 2021, URL: https://docs.microsoft.com/en-gb/azure/active-directory/reports-monitoring/reference-reports-data-retention#how-long-does-azure-ad-store-the-data

Discussions between SLM Rijk and Microsoft have clarified that Microsoft's third row of data includes all system-generated event logs, which Microsoft keeps for six months after the end of the subscription. Microsoft has explained the "*180 days after end of subscription*" represents a maximum back-end retention period. Privacy Company asked if this could mean that Microsoft would retain data for 15 years if an employee joined the organisation in 2016. Microsoft clearly denied: "*Accordingly, the "15 year" example is not reflective of any actual practice. No team would be able to justify retaining their service generated data for 15 years.*"[182]

In the previous DPIA of June 2020 a detailed description was provided of the different (and contradictory) retention periods for the audit logs, Cosmos and the back-ups. This information is not repeated here.

Though Microsoft does not provide a clear list of the different retention periods, it can be assumed that Microsoft stores some Diagnostic Data for a period of 30 days, some other usage data for six months, audit log files registering access to Content Data for at least a year (or 90 days for guest users in the Azure AD), while data in Cosmos can be stored up to 18 months from the moment the data are received by Microsoft.

In reply to this DPIA, Microsoft has explained there is no generalized 18-month retention period for COSMOS. "*The majority of data stored in COSMOS is service generated data, subject to varying retention requirements based on business need. We keep system generated logs for the period necessary for the purpose for which logs are generated, guided by principles of data minimization. Many logs are retained for as little as 30 days.*"[183]

The audit performed by EY at the request of SLM Rijk, as published in March 2021, shows that Microsoft imposes access controls to the employees entitled to access certain clusters. Microsoft also imposes maximum retention periods to the copies used by employees. EY did not verify the quality of the pseudonymisation, or the compliance with the 18 months period.

Microsoft does not offer a possibility to delete outdated Diagnostic Data from Teams, OneDrive or SharePoint on any platform. It is not clear why Microsoft cannot offer this option per device ID, the way Microsoft does offer such an option for Windows 10 Telemetry Data. Microsoft points out that an organisation may delete all historical Diagnostic Data by ceasing to use a user work account in Office 365, and eliminate its Azure Active Directory presence.[184]

During finalisation of this DPIA report, SLM Rijk became aware of a new US fiscal obligation. This Treasury regulation, introduced in 2020, obliges US communication providers to retain IP addresses from end users for 3 to 6 years if they want to deduct Foreign-Derived Income. [185] If this applies to Microsoft, this DPIA will be updated.

---

[182] Microsoft reply to this DPIA, 14 February 2022

[183] Idem.

[184] Ibid, answer Q8b.

[185] Treasury Regulation 1.250(b)-5(e) for services provided to businesses. "*If the location of access cannot be determined (such as where the location of access cannot be reliably determined using the location of the IP address of the device used to receive the service), (…) if gross receipts are at or above this $50,000 threshold, the business recipient's operations that benefit are deemed to be located in the United States*

Part B. Lawfulness of the data processing

The second part of the DPIA assesses the lawfulness of the data processing. This part contains a discussion of the legal grounds, an assessment of the necessity and proportionality of the processing, and of the compatibility of the processing in relation to the purposes.

11. Legal Grounds

To be permissible under the GDPR, processing of personal data must be based on one of the grounds mentioned in Article 6 (1) GDPR. Essentially, for processing to be lawful, this article demands that the data controller bases the processing on the consent of the user, or on a legally defined necessity to process the personal data.

The appropriate legal ground depends on Microsoft's role as (joint) controller, or as processor.

11.1 Diagnostic data Teams, OneDrive, Sharepoint Online and the Azure AD

Thanks to the improved privacy terms that SLM Rijk and SURF negotiated with Microsoft in 2019, Microsoft may only process the personal data it obtains from, through or about the use of its Online Services for three authorised purposes, when proportionate. This purpose limitation should ensure that Microsoft behaves as a data processor for the Diagnostic Data processing. As a processor, Microsoft relies on the legal grounds the controllers have for the three authorised purposes.

As data controllers for the processing of personal data via Teams, OneDrive, Sharepoint and the Azure AD, government organisations and universities can successfully appeal to three of the six possible legal grounds. These grounds apply to three specific purposes for which Microsoft factually acts as data processor: (1) to provide and improve the service, (2) to keep the service up-to-date and (3) secure.

11.1.1 Contract

Article 6 (1) (b) GDPR reads: *"processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."*

Government and university employees are provided with an Office account and Teams, OneDrive and Sharepoint to be able to carry out the tasks included in their job description or to study. Access to these cloud services has become essential to work and study from home. As described in section 6.1 of this report, it is plausible that even after the pandemic has subsided, government organisations and universities continue to have a strong interest in effective online teleworking. Employees and students should be able to access work documents from multiple locations, and on different devices.

To the extent that the processing of the Diagnostic Data from these services is strictly necessary for the performance of the (labour) contract which the data subject has with the government organisation or university, the organisation can successfully invoke this legal ground. This ground only applies to the extent the organisation requires employees and students to use the Microsoft online services to do their work or attend virtual classes for example.

Generally, government organisations also use the Office software to communicate with other data subjects (not employees). Therefore, two other legal grounds need to be considered. These are: (i) the performance of a task carried out in the public interest (Article 6(1) e of the GDPR) and (ii) necessity for the purposes of their legitimate interests (Article 6(1)(f) of the GDPR).

11.1.2 Public interest and legitimate interest

Article 6 (1) (e) GDPR reads: "*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 controller.*"

Article 6 (1) (f) GDPR reads: "*processing is **necessary for the purposes of the legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child**.***

The last sentence of Article 6(1) of the GDPR adds: "*Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.*"

The last sentence of Article 6(1) of the GDPR excludes the application of the legitimate interest ground for processing carried out by public authorities in the performance of their tasks. However, the choice to use certain productivity software is secondary to the performance of public tasks by public authorities, and can therefore also be considered as a task primarily exercised under private law.

As explained in Recital 47 of the GDPR, the legal ground of necessity for the legitimate interest (Article 6(1) f) is more likely to exist *where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.* When Teams is used to communicate with external data subjects (guest users) or the use is mandatory for students, government organisations and universities may also invoke the legal ground of the performance of their public tasks.

Both legal grounds require an assessment of the necessity of the personal data processing, of the proportionality and availability of alternative, less infringing means to achieve the same legitimate purposes (subsidiarity).

Dutch government organisations and universities may process a limited set of Diagnostic Data, without Content Data, on the basis of the necessity for their legitimate interest. This includes processing of Diagnostic Data by Microsoft as a data processor to determine what security updates to serve, and to provide a well-functioning product by troubleshooting and technical error fixing. This legal ground may also be relied upon for the (limited) use of some Diagnostic Data for analytics, as long as the rights and freedoms of the users and other data subjects do not prevail over this interest.

However, this DPIA shows that some Diagnostic Data are or were shared with third parties that are independent data controllers and may process the data for their own marketing purposes. These companies are not contracted as subprocessors by Microsoft. Microsoft is in the process of removing traffic to SharePoint and Cloudflare when an organisation has disabled the Controller Connected Experiences, and admins

are strongly advised to disable access to third party applications in the Teams store. See Section 2.3 for the details.

As this transfer of personal data to third parties (including Microsoft as a data controller) was unintentional, it is certainly not necessary. Nor Microsoft nor the public sector organisations can appeal to the ground of necessity for a legitimate interest for these transfers.

11.2 Telemetry data Office for the Web and *Required Service Data*

As described in Section 5.5 government and university administrators have no control at all over the telemetry events from Office for the Web: they cannot minimize the level, they cannot inspect the data with a Data Viewer Tool or equivalent tool, and Microsoft does not provide access in response to a Data Subject Access Request. Similarly, admins cannot prevent Microsoft from collecting readable usernames in incidental telemetry events about the use of OneDrive. Microsoft has provided explanations about the necessity of the data collection, and has argued that many of these events do not contain personal data. However, in order to prevent a factual qualification as joint controllers with the Enterprise and Education customers, these reassurances need to be independently verified, and Microsoft should be more transparent about this processing.

11.3 Controller Connected Experiences

Even if an admin centrally blocks access to the Controller Connected Experiences, this setting did not yet consistently work in all apps on all platforms. It did not prevent Microsoft's search engine Bing from collecting personal data in SharePoint Online, nor did it prevent traffic to Cloudflare on Microsoft's support website. As explained in Section 5.4.1, the data processing is not necessary and in breach of Microsoft's privacy commitments.

Nor the government organisations and universities, nor Microsoft can appeal to any legal ground for this processing for other purposes than the authorised three processor purposes.

11.4 Analytics & reports in Teams and Viva Advanced Insights

For the Analytics & reports function in Teams, as well as for the use of Viva Advanced Insights (which includes Workplace Analytics), universities and government organisations can only use the legitimate interest as a legal ground. Public law does not require these organisations to collect and use detailed analytics about employee and student behaviour in communication tools such as Teams, or keep track of user interactions with documents on OneDrive or SharePoint. Therefore, the legal ground of necessity for the public interest cannot be successfully invoked.

In order to rely on the last ground of legitimate interest, the interests of the organisations and the data subjects must be carefully weighed. Both analytic functionalities can be used as an employee (or student) monitoring system, certainly in combination with usage reports from the Admin 365 Center. Microsoft by default enables the full functionality of Teams Analytics & reports. If the organisation does not apply specific policy rules the processing will have a considerable impact on the rights of the data subjects. The fundamental rights and interests of employees and students are likely to outweigh the interests of the government organisations and universities if the organisations do not first assess the necessity of this processing.

Even if an organisation finds some analytics to be necessary, the purposes for use must be clearly defined in transparent policy rules.

This report therefore repeats the recommendation from June 2020 that government organisations and universities must perform a DPIA before they decide to use (in fact: actively disable) analytic services such as the Office 365 Reports in the Admin Center, MyAnalytics, Delve, Workplace Analytics and the new Teams Analytics & reports. Such a DPIA should take the risk into account that the use of these analytics may have a strong chilling effect on employees. The organisations must consider that Teams, OneDrive and SharePoint are seldom used in isolation. Inevitably, employees and students spend many working hours with the productivity software of Microsoft (Office, Windows and other services and applications).

Because Microsoft delivers the Teams Analytics & reports service by default with all surveillance options enabled (see Figure 11) , Microsoft also factually determines the purpose of this processing, and behaves as a joint controller. Microsoft does not explain what the result is of the pseudonymisation choice offered to admins: does this also have an impact on the raw Diagnostic Data held by Microsoft? Absent such information and absent privacy by default, nor the government organisations and universities, nor Microsoft can appeal to any legal ground for this processing.

In sum, contrary to Microsoft's privacy commitments, it has not yet effectively limited the purposes for the processing of all Diagnostic Data. When Microsoft is a joint controller with the government organisations and universities, neither parties have a legal ground for the processing.

12. Special categories of data

As explained in section 2.7.1 of this DPIA, it is up to the individual government organisations to determine if they process special categories of data, in the contents of Teams conversations or files stored on SharePoint or OneDrive, or in the Account, Support and Diagnostic Data.

Special categories of data are *data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation or data relating to criminal convictions and offences.*

The technical analysis shows that there are no significant changes in the processing by Microsoft that would result in new or unexpected processing of these sensitive and special categories of data. Therefore, the analysis in the DPIA from June 2020 is not repeated here.

13. Purpose limitation

The principle of purpose limitation is that data may only be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*" (Article 5 (1) (b) GDPR). Essentially, this means that the controller must have a specified purpose for which he collects personal data, and can only process these data for purposes compatible with that original purpose.

Data controllers must be able to prove, based on Article 5(2) of the GDPR, that they comply with this principle (accountability). As explained in section 5.3 of this report only data controllers may take decisions about the purposes, including the decision to transfer data to third parties to process the data for additional purposes. As data processor, Microsoft may not process the personal data for other than the three authorised purposes. Microsoft's Office 365 customers should be able to rely on the contractual guarantees and privacy controls to prevent any personal data from being processed beyond these authorised purposes. This was not yet the case. Most of the processing for unauthorised purposes observed in this DPIA seemed incidental, a bug instead of a feature. However, Microsoft should be able to prevent such incidents, by systematically checking its own tools and products, and verifying compliance with the processor contract.

One example of data processing for an intended new purpose is the new Analytics & reports functionality in Teams. The functionality is designed to provide insights to admins in the Teams use by identifiable individuals. This is a form of further processing of the personal Diagnostic Data of employees and students. As Microsoft has turned On all options by default, the tool can easily be turned into an employee monitoring system. Only controllers may decide to (further) process the Diagnostic Data for such a new purpose, not Microsoft in its role as data processor. The processing for this purpose cannot be considered *compatible* with the three authorised purposes.

14. Necessity and proportionality

14.1 The principle of proportionality

The concept of necessity is made up of two related concepts, namely proportionality and subsidiarity. The personal data which are processed must be necessary for the purpose pursued by the processing activity. Proportionality means the invasion of privacy and the protection of the personal data of the data subjects is proportionate to the purposes of the processing. Subsidiarity means that the purposes of the processing cannot reasonably be achieved with other, less invasive means. If so, these alternatives have to be used.

Proportionality demands a balancing act between the interests of the data subject and the data controller. Proportionate data processing means that the amount of data processed is not excessive in relation to the purpose of the processing. If the purpose can be achieved by processing fewer personal data, then the controller needs to decrease the amount of personal data to what is necessary.

Therefore, essentially, the data controller may only process the personal data that are necessary to achieve the legitimate purpose, but may not process personal data he or she may do without. The application of the principle of proportionality is thus closely related to the principles of data protection from Article 5 GDPR.

14.2 Assessment of the proportionality

The key questions are: are the interests properly balanced? And does the processing not go further than what is necessary?

To assess whether the processing is proportionate to the interest pursued by the data controller(s), the processing must first meet the principles of Article 5 of the GDPR.

As legal conditions they have to be complied with in order to make the data protection legitimate.[186]

Data must be '*processed lawfully, fairly and in a transparent manner in relation to the data subject*' (Article 5 (1) (a) GDPR). This means that data subjects must be informed about the processing of their data, that all the legal conditions for data processing are adhered to, and that the principle of proportionality is respected.

Microsoft has promised to the Dutch government and universities to increase transparency about the Diagnostic Data in a number of ways:

- Publish adequate documentation about the telemetry events and the log files generated on its cloud servers;
- Create effective Data Viewer Tools for all core online Office services;
- Improve replies to Data Subject Access Requests, by better supporting admins in disclosing the Diagnostic Data or explain why it cannot provide access.

This DPIA shows that Microsoft does not live up to these promises yet.

First, there is only a description, but no event-level documentation on the Office for the Web telemetry. Even when telemetry is set to the minimum level of 'Neither', this DPIA shows that Microsoft still generates 100 different telemetry events about the three tested applications on the five platforms. Only 10% of these events is publicly documented, and due to spelling differences, many event names do not match with the names in the published documentation. Because of this lack of transparency, customers have no way of verifying what personal data Microsoft collects, and whether that complies with the chosen data minimisation settings. Admins and end users are literally kept in the dark about the nature of this data processing.

Second, though Microsoft has improved the Data Viewer Tool for Teams and OneDrive, it is not yet available for OneDrive on Windows and MacOS. Microsoft does not plan to make an end user transparency tool available for any Office for the Web apps. It cannot use the DDV, as this telemetry stream is not created by the telemetry client installed on the end user device.

Third, Microsoft's DSAR tool for access to the telemetry events did not generate easily understandable output. Privacy Company was unable to effectively compare the produced data with the captured Telemetry Data from the network traffic. This was due to post-processing by Microsoft of the raw telemetry events. For example, in the produced results Microsoft removed the names of the telemetry events, while these names were instrumental in comparing the collected versus the provided Diagnostic Data. This makes the DSAR for Diagnostic Data unreliable as a transparency tool to

[186] See for example CJEU, C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ECLI:EU:C:2014:317. Paragraph 71: *In this connection, it should be noted that, subject to the exceptions permitted under Article 13 of Directive 95/46, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive (see Österreichischer Rundfunk and Others EU:C:2003:294, paragraph 65; Joined Cases C-468/10 and C-469/10 ASNEF and FECEMD EU:C:2011:777, paragraph 26; and Case C-342/12 Worten EU:C:2013:355, paragraph 33).*

verify the scope of the diagnostic data processing. Microsoft explained, as quoted in Section 2.5, that many data are not personal data, or retained too short to be shown in a DSAR request. However, these statements need to be independently verified.

Only because of the network interception it was discovered that Microsoft does collect directly identifiable usernames in certain OneDrive events. This data collection may well be necessary to offer a well-functioning service, but Microsoft did not tell its customers. Absent transparency through either the DDV or the DSAR for telemetry events, Microsoft needs to reassure its customers in another way about the proportionality of the data processing, by organising an independent audit on the contents of the collected telemetry events.

In sum, Microsoft does not yet meet the required and agreed transparency standard. The lack of transparency makes the data processing inherently unfair.

The principles of data minimisation and privacy by design require that the processing of personal data be limited to what is necessary. The data must be *'adequate, relevant and limited to what is necessary for the purposes for which they are processed'* (Article 5(1)(c) of the GDPR). This means that the controller may not collect and store data which are not directly related to a legitimate purpose. According to this principle, the default settings for the data collection should be set in such a way as to minimise data collection by using the most privacy friendly settings.

Microsoft does offer some controls to admins to minimise the processing of personal data. Administrators can set the telemetry level to 'Neither' (on 4 of the 5 platforms, but not in Office for the Web) and centrally disable use of the Controller Connected Experiences. They can also block traffic to third parties in the Teams store, and effectively block the use of Giphy (now that Microsoft also prevents personal data from being sent to Giphy due to incoming images from external users). In the Teams Analytics & reports tool, administrators can disable direct identifiers (choose pseudonymisation). As shown in this DPIA, none of these data minimisation options are effective on all platforms. With Teams Analytics, it is not clear if the pseudonymisation choice has any influence on raw data processed by Microsoft.

The principle of storage limitation requires that personal data should only be kept for as long as necessary for the purpose for which the data are processed. Data must *'not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed*' (Article 5(1)(e), first sentence, GDPR). This principle therefore requires that personal data be deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller. The text of this provision further clarifies that '*personal data may be kept longer in so far as the personal data are processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1), subject to the implementation of appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject'* (Article 5(1)(e), second sentence, GDPR).

As explained in Section 10 (*Retention periods*), Microsoft retains the Diagnostic Data for 30 days up to a maximum of 18 months after the initial collection (as agreed in the privacy amendment with SLM Rijk). These data will be processed in the EU after completion of the EU Data Boundary, with the exception of the incidental transfer of Security Data.

The Telemetry Data should only contain a very limited set of pseudonymous identifiers if the administrator settings are set to 'Neither' and the Controller Connected Experiences are switched off. Microsoft has explained it will retain the exceptional OneDrive telemetry events (which may contain directly identifiable data), only for a short period of time, and not process these any further. However, Microsoft should enable admins to verify the contents of this data stream, by publishing a list of telemetry endpoints and their function, including an explanation about the specific endpoint for the specific OneDrive telemetry data that contain readable usernames and path names.

The system generated log files on the other hand are designed to register all access to Content Data (by customers and by Microsoft). These logs contain much more information, directly identifiable user data and snippets of content. Different from the telemetry events, there is a clear security purpose to retain these logs in an identifiable format for the default period of 1 year. This period can be extended by admins if that is necessary for their own compliance process. These log files are only processed and stored in the EU, where the logs are generated.

There is a third category of usage logs with personal data, accessible via the Admin 365 Center, for which the retention periods are unclear.

Absent clear and easily accessible documentation from Microsoft about the retention periods, their necessity and controls for admins to actually determine the retention periods, it cannot be assessed if Microsoft's current retention policy is proportionate.

In sum, though Microsoft has fixed some apparent bugs, the current data processing of the Diagnostic Data is still not sufficiently transparent, nor sufficiently respectful of the legal privacy by design requirements. Therefore, government organisations and universities cannot adequately determine the proportionality of the processing.

14.3 Assessment of the subsidiarity

The key question is whether the same goals can be reached with less intrusive means.

Since 2019 Microsoft has made major improvements in offering admins options to limit the amount of personal data processing (the Diagnostic Data including the Telemetry Data), limit the purposes for the processing and improve transparency.

Purpose limitation, transparency, and the ability for admins to minimise the processing, are essential to reduce the intrusiveness of the processing. If all privacy options functioned as documented, and the resulting traffic could be compared with public documentation, the privacy impact for data subjects would be limited. It follows from the public DPIA from SLM Rijk and the University of Groningen with the Hogeschool Amsterdam on Google Workspace that the Google cloud communication and storage services cannot be considered a less intrusive alternative.[187]

This report does not include an analysis of other available communication and data storage tools that may present less data protection risks. This can be the case if they are hosted locally (*on premises*), are offered by EU companies without subsidiary in

[187] DPIA on Google Workspace, 12 February 2021, URL: https://www.rijksoverheid.nl/documenten/publicaties/2021/02/12/google-workspace-dpia-for-dutch-dpa. See also the Update DPIA from August 2021, URL: https://www.surf.nl/files/2021-08/update-dpia-report-2-august-2021.pdf

the USA, or because, as open-source tools, their compliance with the GDPR can be more easily assessed. Organisations that wish to explore such alternatives, are advised to follow the initiatives from the French Data Protection Authority CNIL to assist organisations to help identify possible alternatives.[188]

With regard to Teams Analytics & reports admins can choose to pseudonymise the usage data. Reporting with aggregate statistic may be less intrusive, but every organisation first needs to determine the necessity for this type of analytics. The organisation must also assess if it has a legitimate purpose to monitor individual employee behaviour, preferably by comparing this Teams functionality with the use of other available Analytic tools from Microsoft for Windows and Office services.

15. Data Subject Rights

The GDPR grants data subjects a number of privacy rights. In this section, only two of these rights are discussed, because there are relevant changes compared to the June 2020 DPIA. These are the right to information and the right to access.

Right to information

Data subjects have a right to information. This means that data controllers must provide people with easily accessible, comprehensible and concise information in clear language about, inter alia, their identity as data controller, the purposes of the data processing, the intended duration of the storage and the rights of data subjects.
As assessed in Section 14.2 above, the information Microsoft provides about the Diagnostic Data processing is incomplete. Without this information, nor admins nor end users can fully understand what personal data are processed and for what purposes.

Right to access

Secondly, data subjects have a (fundamental) right to access personal data concerning them. Upon request, data controllers must inform data subjects whether they are processing personal data about them (directly, or through a data processor). If this is the case, they must provide data subjects with a copy of the personal data processed, together with information about the purposes of processing, recipients to whom the data have been transmitted, the retention period(s), and information on their further rights as data subjects, such as filing a complaint with the Data Protection Authority.

Microsoft undertakes as a data processor "*to redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Online Service. Microsoft shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.*"[189]

[188] CNIL, CNIL calls for changes in the use of US collaborative tools by French universities, 31 May 2021, URL: https://www.cnil.fr/en/cnil-calls-changes-use-us-collaborative-tools-french-universities

[189] Microsoft Online Services Data Protection Addendum, 15 September 2021, URL: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA , p. 7.

As a data processor, Microsoft provides different tools for administrators to search and export all data that Microsoft considers to be a user's personal data. These tools and their outputs are described in Section 2.5. [190]

Microsoft refuses to provide access to the Telemetry Data it collects via (any) Office for the Web app, and does not provide any access to Diagnostic Data about the use of (Processor) Connected Experiences, as they are part of the category of '*Required Service Data*'. In the last improvement plan from June 2020 agreed with SLM Rijk, Microsoft committed to expand its DSR tool and provide clear explanations in cases where it could not provide the requested access. Microsoft's explanations are quoted in Section 2.5. Of course, Microsoft does not need to provide access to data that are not personal data, but these statements will have to be verified.

Though Microsoft has made a Diagnostic Data Viewer Tool available for Teams and OneDrive on most platforms, Microsoft does not explain why there is no such tool for OneDrive on MacOS and Windows. Since the tool only shows approximately 10% of the telemetry events (the rest are '*Required Service Data*' according to Microsoft), the tool is not a reliable instrument for verification.

In sum, government organisations are currently not in a position to (fully) honour the rights of data subjects.

[190] There is another possibility to look at (a small part of) the Diagnostic Data per user, via Activity Reports in the Microsoft 365 Admin center. This possibility has not been explored in this report. Data subjects can also see part of the analyses that Microsoft performs based on the system-generated event logs about their use of Office 365, Exchange Online and SharePoint Online and OneDrive via Delve and MyAnalytics. This report recommends performing a DPIA before using these services. Therefore, these tools are not discussed as standard options to obtain access.

Part C. Discussion and Assessment of the Risks

This part of the DPIA contains a discussion and assessment of the risks for data subjects related to the processing of Diagnostic Data from Teams, OneDrive, Sharepoint Online in combination with the Azure AD. This part starts with an overall identification of the risks in relation to the rights and freedoms of data subjects, resulting from the processing of information about their use of, and behaviour in, the tested three applications.

16. Risks

16.1 Identification of Risks

The processing of personal data about the individual use of Teams, OneDrive, and Sharepoint results in a number of risks that are related to the processing of metadata. This DPIA is focussed on the risks caused by the processing of Diagnostic Data. However, it is inevitable to also discuss the risks caused by the possible undue access to Content Data by US government authorities, since Microsoft is a US based company.

16.1.1 Metadata

Both Microsoft and the government organisations / universities can use the collected Diagnostic Data about the user to create a profile of the user. Microsoft has access to more personal data about the use of the Azure AD and the use of Teams, OneDrive and SharePoint through Telemetry Data and raw data logs generated on its cloud servers Data than admins can see and export from the available reports and logs. This leads to a risk that data subjects cannot exercise their fundamental right to access these personal data.

As a result of the Covid-pandemic, workers spend considerable amounts of work time using videoconference tools. That makes processing for such employee profiling purposes more plausible. The knowledge that employers (government organisations and universities) can process the Diagnostic Data for profiling purposes can cause a *chilling effect* on employees and students using Teams. A *chilling effect* is the feeling of pressure someone can experience through the monitoring of his or her behavioural data, discouraging this person from exercising their rights, such as accessing certain content.[191] Government and university employees and students may feel unable to exercise their right to (moderately) make use of employer and study facilities without being observed and to communicate about private affairs, such as videoconferencing with a friend or family member. Employees may also feel unable to exercise their right to whistle blow, for example by organising a conference call with members of the Workers Council or Union.

16.1.2 Content Data

Organisations should be aware, when they assess the risks of the use of a public cloud service for video conferencing and online file storage, of the possible undue access to these data by US government authorities. Stored or exchanged data may contain privacy-sensitive datasets, special categories of data, confidential government information or state secrets (Classified Information). Unauthorised access to such

[191] Merriam-Webster Online Dictionary, "chilling effect", URL: https://www.merriam-webster.com/legal/chilling effect.

sensitive or classified data could for example lead to a risk of being profiled as a high-risk person, being blacklisted, or blackmailed. To completely mitigate these risks, organisations should encrypt all data, have exclusive control over the encryption keys and have access to the source code of the applications to exclude the presence of backdoors. If that is not possible, and the risk assessment still allows for the use of these applications, organisations must apply all available encryption tools, including tools where the provider has theoretical access to the keys.

Additionally, there are internal risks of unauthorised access to the data. To mitigate these risks, organisations must create policy rules for the Content Data, such as what type of Content Data may be shared internally and externally, determine retention periods for the stored data, and set rules when conference calls may be recorded, and for what purpose(s).

16.2 Assessment of Risks

The risks can be grouped in the following categories:

- Inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage[192]

These risks have to be assessed against the likelihood of the occurrence of these risks and the severity of the impact.

The UK data protection commission ICO provides the following guidance: "*Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.* [193]

[192] List provided by the ICO, How do we do a DPIA, Step 5: How do we identify and assess risks?, URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/ .
[193] Idem.

In order to weigh the severity of the impact, and the likelihood of the harm for these generic risks, this report combines a list of specific risks with specific circumstances of the specific investigated data processing.

16.2.1 Loss of control, loss of confidentiality: undue access by US government authorities to sensitive and special categories of personal data in the Content Data

Microsoft does not offer a possibility to apply E2EE to group meetings and chats in Teams.[194] This means there is a chance that Microsoft is compelled to intercept these data and lift its own encryption. Similarly, if an organisation does not encrypt stored data in OneDrive and SharePoint with its own keys, there is a chance that US law enforcement, courts or secret services may compel Microsoft to disclose these data. As shown in the DTIA performed as part of this DPIA, the likelihood that this risk will manifest is very slim.

The impact of such undue access depends on the nature of the data. If the data are effectively anonymised or already public, the impact is low. With pseudonymised or regular personal data, the impact increases, but the privacy risks for data subjects are still assessed as low, due to the mitigating measures taken by Microsoft, including encryption with keys provided by Microsoft.

In view of Microsoft's historical disclosure data, comparison with transparency reports from other cloud providers, and Microsofts commitment to legally fight every order and compensate its customers, the likelihood of the occurrence of undue access by US law enforcement agencies to the Content Data is very low. Even if the likelihood of occurrence is extremely low, the impact on data subjects in case of disclosure of their sensitive and special categories of personal data to US law enforcement or security services can be extremely high. This is due to the lack of notification and the lack of an effective means of redress for EU citizens. This risk even occurs when these data are exclusively processed and stored in the EU, because access to these data can be ordered through US legislation such as the US CLOUD Act. Hence, there is a high risk for the processing of sensitive and special categories of data via Teams, OneDrive, and SharePoint, as long as the organisation cannot control its own encryption keys.

16.2.2 Loss of control: undue access by US government authorities to Diagnostic Data

Microsoft's current structural transfer of Telemetry Data to the USA poses data protection risks, due the chance of undue access by US government authorities. The impact on data subjects is mitigated because Microsoft only collects pseudonymised identifiers. Additionally, organisations can minimise the collection of Telemetry Data, by selecting the lowest level of 'neither', and are advised never to include personal data in file and path names. It follows from the risk calculation in the DTIA that the likelihood is very small that Microsoft will be compelled to disclose these data to US government authorities. These risks can be accepted, as these risks will be mitigated by the end of 2022 the latest, upon completion of Microsoft's EU Data Boundary. This means that Microsoft will automatically and exclusively collect, process and store the Content Data, the Diagnostic Data, as well as the Account Data and the Support Data from its EU Enterprise and Education customers in Microsoft's EU data centres.

[194] Though Microsoft has rolled-out E2EE for unscheduled one-to-one video calls globally since November 2021, this functionality was not yet available in the Dutch government and business licenses in January 2022, and has not been tested.

To further mitigate some of the risks of unlawful further processing in the USA, government organisations and universities can create policy rules to prevent Microsoft from processing confidential or sensitive data through the Diagnostic Data. They could for example draft a policy to prohibit the use of directly identifying personal or confidential data in file- and path names. Depending on the sensitivity and confidentiality of the data, they may want to apply additional data minimisation measures, such as using pseudonyms in the Azure AD, and ensuring through Azure AD conditional access that guest users accept the organisation's privacy conditions.

Overall, in view of Microsoft's measures, its transparency reporting, the announcement of the EU Data Boundary for all personal data in the Core Online Services, and provided the organisations and universities apply the recommended data minimisation measures, the likelihood of the occurrence of undue access by US law enforcement agencies to the Diagnostic Data is very low. The consequences for data subjects can vary from low to very serious. This results in a low risk for data subjects, pending a possibly different future risk assessment by the EDPS.

As mentioned in Section 10, Microsoft may be obliged to retain IP addresses from end users for 3 to 6 years, as evidence that the income was earned in the EU. Microsoft was still inquiring if this obligation applies when this DPIA was finalised. If this obligation applies to Microsoft, this DPIA will be updated.

However, even after completion of its EU Data Boundary for its core Online Services and Support requests from EU customers, Microsoft will continue to incidentally transfer some personal diagnostic data to the USA for security purposes. Though Microsoft takes many steps to first pseudonymise and aggregate these data about threats and malicious activities on customer' servers and end user devices, prior to the transfer, Microsoft can still transfer pseudonymous personal data such as device identifiers and IP addresses to its centralised security monitoring and logs.

As a data processor, Microsoft must take adequate security measures to protect the personal data of its customers. In view of the legitimate purpose of the processing, to recognise and mitigate security risks for all other end users and customers, it is necessary for Microsoft to operate a central Network Operations Centre. It is plausible that Microsoft cannot perform these tasks in separate regionalised security teams, as bad actors may be located anywhere in the world.

The chances that the personal data of a particular data subject are included in these incidental transfers, are small. Therefore, the occurrence of the risk of these incidental security transfers can be assessed as low, even though the impact could be very high.

16.2.3 Ongoing incidental transfer of usernames / e-mail addresses / pathnames OneDrive to the USA

At the lowest telemetry level 'Neither' Microsoft should only collect pseudonymised personal data, no Content Data or usernames. However, readable usernames and file names were observed in OneDrive URLs in telemetry events. Microsoft has explained that this is an exception on its guarantee that the *Required Service Data* do not contain directly identifiable (readable) usernames/mail addresses. As evidenced by the technical network traffic analysis performed for this DPIA, Microsoft can collect the username and/or email address of an employee, together with the tenant's name and the file path with the full name of the document. Microsoft has explained why this is exceptionally necessary in OneDrive, for example in case multiple users simultaneously access the same document. Microsoft has also explained that access to these OneDrive Diagnostic Data is audited, limited to just-in-time security group,

and limited to engineers that have an approved business justification. Additionally, none of these data are retained longer than 30 days.

In view of these mitigating measures, and pending an audit on the contents of the *Required Service Data*, the privacy risks for data subjects can be qualified as low.

16.2.4 Lack of transparency Telemetry Data

Microsoft is not transparent at all about the collection of Telemetry Data in Office for the Web (when users access the Office apps through the browser), and most of the events collected from the installed apps at the lowest telemetry level of 'Neither'. In reply to this DPIA, Microsoft explained that these events are only collected when strictly necessary, and are too dynamic, too costly to document. The browser telemetry events cannot be shown in the Diagnostic Data Viewer (DDV), as they are collected via the browser, and not via the in-built telemetry client in the installed Office applications. Microsoft has explained that telemetry data that are not shown in the DDV are part of a category called *Required Service Data*. The technical analysis shows that there are no significant changes in the processing by Microsoft that would result in new or unexpected processing of these telemetry events. Microsoft has confirmed it only processes these data for the three agreed processor purposes. Pending an audit on the contents of the *Required Service Data*, the privacy risks for data subjects can be qualified as low.

16.2.5 Inability to exercise data subject access rights to Required Service Data

During the tests performed in May 2021, the DDV was only functional for telemetry events created by the Teams app on Android. The re-tests in January 2022 show that the DDV is now available on all platforms for Teams, and on the two mobile platforms for OneDrive. However, the majority of events belongs to *Required Service Data*, and are not shown in the DDV. This makes the DDV an unreliable tool for data subject access requests. However, Microsoft offers other tools to admins to obtain detailed information about the contents and metadata logged about individual use of Teams, OneDrive, SharePoint and the Azure AD. Unfortunately, the search query for the Diagnostic Data does not generate easily understandable output. Privacy Company was unable to effectively compare the produced data with the captured Telemetry Data from the network traffic. This was due to post-processing by Microsoft of the raw telemetry events. For example, in the produced results Microsoft removed the names of the telemetry events, while these names were instrumental in comparing the collected versus the provided Diagnostic Data.

Microsoft explained to SLM Rijk that there are three reasons why the query for the Diagnostic Data does not produce all observed telemetry events in the network traffic. Microsoft immediately deletes some events, quickly removes the identifiers that would allow for identification, or does not collect any personal data at all with some other events. Additionally, Microsoft has committed to improve it take out tool for the Diagnostic Data, to better assist administrators with any data subject access requests from individual employees. In view of this explanation and this commitment, the risks for data subject can be assessed as low.

16.2.6 Lack of control: personal data shared with Microsoft and third parties as controllers

In May 2021, traffic to third parties was observed. Such third parties are not bound by the data processing agreement with the Dutch government and Dutch universities, and may process these personal data for their own (commercial) purposes. Microsoft has since taken mitigating measures, or enables administrators to prevent this traffic.

Microsoft has ensured that even guest users cannot cause traffic to Giphy in Teams, and enables administrators to block traffic to third parties via the Teams app store by only allowing Microsoft apps.

Microsoft is in the process of structurally eliminating traffic to its search engine Bing from SharePoint when an Enterprise or Education customer has disabled the Controller Connected Experiences. The removal of traffic to Bing from SharePoint should be completed by July 2022.
Finally, Microsoft committed to remove all traffic to Cloudflare if a customer has disabled the Controller Connected Experiences, as Cloudflare is not an authorised subprocessor of Microsoft. Yet, as retested in January 2022, when end users are linked to Microsoft Support pages from within Office applications, there is still traffic to Cloudflare.

Assuming Microsoft will definitely terminate the unauthorised traffic to Cloudflare and to itself as controller for Bing, and assuming the organisations will block access to the third-party apps in the Teams app store, the risks of unlawful processing for purposes other than the three authorised purposes instructed by the government organisations and universities, are low. That is why the privacy risks for the data subjects are low.

16.2.7 Employee monitoring system: chilling effect

Microsoft offers two distinct analytics services for Teams: Teams Analytics & reports and Viva Insights. The first tool (Teams Analytics & reports) is enabled by default, and provides detailed insights to admins about individual working behaviour. Based on the reports, managers could create comparisons between employees regarding their use of Teams, including the number of messages, calls, group chats, etc. The reported items include time stamps. These allow for a detailed insight in the productivity and availability of an individual employee. The knowledge that their employer can process these data for evaluation purposes can have a *chilling effect* on Teams users. This can infringe on their privacy rights, and impede their exercise of related fundamental rights such as the freedom to send and receive information Though Microsoft offers a possibility to pseudonymise the names of the employees, it is not clear if this has any effect on Microsoft's raw data logs.

The other tool, Viva Insights is configured disabled by default. This tool includes MyAnalytics and Workplace Analytics, tools that respectively offer employees information about their productivity, and offer managers insights in individual employee work patterns. If an administrator explicitly enables the service, the individual user still has the option to opt-out. If admins would enable these tools, they have to take into account that the Viva Advanced Insights are generated and processed in the USA, regardless of the geolocation choice for the EU.

Assuming the government organisations and universities follow the recommendations of SLM Rijk and SURF not to use these tools, the risks for data subjects are low. If they do want to use these analytic tools, they must conduct a DPIA and create a policy with specific rules about the purposes for which these identifiable analytic insights and reports may be processed.

16.3 Summary of risks

These circumstances and considerations as explained above lead to the following single high, and six low data protection risks for data subjects:

1. Loss of control, loss of confidentiality: undue access by US government authorities to Content Data

2. Loss of control: undue access by US government authorities to Diagnostic Data
3. Ongoing incidental transfer of usernames / e-mail addresses / pathnames OneDrive to the USA
4. Lack of transparency Telemetry Data
5. Inability to exercise data subject access rights to *Required Service Data*
6. Lack of control: personal data shared with Microsoft and third parties as controllers
7. Employee monitoring system: *chilling effect*

Based on the ICO model, this results in the following matrix:[195]

Severity of impact	Serious harm	**Low risk 1[196], 2, 3, 7**	**High risk**	**High risk**
	Some impact	**Low risk 6**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk 4, 5**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm (occurrence)		

[195] Copied from the DPIA guidance from the UK data protection commission, the ICO. URL: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-carry-out-a-dpia/

[196] As assessed in the DTIA, based on the guidance from the European Data Protection Board, even though the occurrence of the risk of undue access is assessed as extremely low, the impact on data subjects is very high in case of sensitive or special categories of data. This is not correctly reflected in this table.

Part D. Description of risk mitigating measures

Following the Dutch government's DPIA model, Part D describes the proposed countermeasures against the data protections risks identified in part C.

The following section contains a table of the mitigating technical, organisational and legal measures that can be taken by the government organisations/universities, and by Microsoft.

17. Risk mitigating measures

In section 16.2 of this report, seven privacy risks for data subjects have been discussed. There six low risks, plus a high risk if organisations use Teams, OneDrive and SharePoint to exchange/store sensitive and special categories of data without applying encryption with their own keys. The government organisations and universities must take the recommended measures to ensure that there are only low risks for data subjects, through a combination of technical and organisational measures. Microsoft must execute some mitigation measures it has already committed to, and is advised to take some additional measures.

17.1 Measures against the one high and six low risks

The table below show the single high, and six low data protection risks for data subjects, with the mitigating measures government organisations, universities and Microsoft can take.

No.	High risk	Measures government organisations and universities	Measures Microsoft
1.	Content Data processed in the EU accessible for Microsoft if not E2EE	Do not exchange sensitive or special categories of data via Teams calls that are not end-to-end encrypted	Commit to a clear deadline when E2EE will be supported for group meetings and chat
		Use Double Key Encryption for documents with sensitive or special categories of data stored in SharePoint/OneDrive. This includes recordings of Teams meetings. Use Customer Key and Customer Lockbox for other stored personal data	
		Enable E2EE for Teams 1-on-1 calls by default, and instruct end-users to also enable E2EE	
		Enable E2EE in Teams for all meetings and chats as soon as Microsoft makes this available	Comply with the SCC requirement to inform customers when Microsoft can no longer comply with the data protection guarantees in the SCC

		Create a Teams and OneDrive privacy policy for internal users and guest users, set rules for sharing of files and images. Make employees and guest users accept these rules through Terms & Conditions imposed by Azure AD	
No.	Low risks	Measures government organisations and universities	Measures Microsoft
2.	Structural transfer of Telemetry Data to the USA (until December 2022)	Accept the temporary risk of the transfer of these pseudonymised data while Microsoft is developing the EU Data Boundary	Apply EU Data Boundary to all personal data by the end of 2022 the latest (with known exceptions)
	Possible access from the USA to audit logs, Azure AD and Telemetry Data processed and stored in the EU after 2022	Accept the risk of access to names and e-mail addresses in the Azure AD or consider the use of pseudonyms in the Azure AD.	Inform customers about the actual status per service of the EU Data Boundary
		Don't use SMS for authentication to prevent the transfer of unencrypted mobile phone numbers to third countries. Instead, use the Authenticator app or a hardware token	
		Use pseudonyms when the Azure AD is used for Single Sign On with external suppliers for employees whose work identity must remain confidential	
	Incidental transfers of pseudonymous data to the USA for security purposes	When using OneDrive and SharePoint, establish policies to prevent file names and file paths from containing personal data	
3.	Ongoing incidental transfer of usernames / e-mail addresses / pathnames on OneDrive to the USA	Consider the use of pseudonymous accounts for employees whose work identity must remain confidential	
		When using OneDrive and SharePoint, establish policies to prevent file names and file paths from containing personal data	
4.	Lack of transparency Telemetry Data	Regularly use the Data Viewer Tool when available, and compare the results with Microsoft's public documentation	Provide a functional Data Viewer Tool for OneDrive telemetry data on Windows and MacOS

		Use Microsoft's DSAR tool for admins to obtain access to diagnostic data, and compare with an occasional network traffic analysis	Verify compliance with purpose limitation by adding specific audit questions about the contents, use purposes and retention periods of *Required Service Data*.
		Inform employees about their access possibilities via the Data Viewer tool, or by filing a DSAR with the admin of the organisation	Provide more information on the *Required Service Data*, including Office for the Web
5.	Difficulty to exercise data subject access rights to *Required Service Data*	Use Microsoft's DSAR tool to obtain access to diagnostic data, and compare with an occasional network traffic analysis	Improve the DSAR tool for Diagnostic Data
		Support a specific audit by SLM Rijk on Microsoft's collection and use of the *Required Service Data*	Provide a clear and understandable explanation about the contents of the *Required Service Data*
			Let auditors independently verify the explanation why the DSAR tool provides very limited access to *Required Service Data*: data no longer stored, or no personal data collected
6.	Lack of control: personal data shared with Microsoft and third parties as controllers	Disable Additional Optional Connected Experiences (Microsoft as controller)	End of Q2 2022: all traffic to Bing removed from SharePoint Online
		Disable access to third party apps in the tab in Teams	Do not send traffic to Cloudflare on Microsoft support pages that are accessed from links in Teams settings on the different platforms
		Instruct end users not to use Bing image searches in SharePoint Online (until functionality is removed)	
7.	Employee monitoring system: chilling effect	Turn off functionality in Teams Analytics & reports, use pseudonymisation: do not enable Viva Insights	Comply with art. 25 GDPR privacy by default: disable Teams Analytics & reports by default
		Conduct DPIA prior to use of the analytics tools such as Viva and Teams Analytics & reports, certainly when used in combination with other Microsoft Windows & Office Analytical services	

		Create a policy to prevent use of Teams Analytics & reports as an employee monitoring tool	When an admin opts-in to pseudonymise the data, inform about the consequences for the raw data held by Microsoft

17.1.1 Measures Microsoft to mitigate the risks

- Ensure that the EU Data Boundary is completed by the end of 2022 as announced. Inform Enterprise and Education customers about the actual status per service of the EU Data Boundary, and ensure that all related personal data are exclusively processed in the EU, once available.

- Provide a functional Data Viewer Tool for OneDrive telemetry data on Windows and MacOS.

- Provide more public information on the nature of telemetry events generated by the use of Office for the Web.

- In view of the lack of transparency about the *Required Service Data*, Microsoft should organise an independent audit on the contents of these data, to verify compliance with purpose limitation and retention periods in the privacy amendment with the Dutch government and universities.

- Improve the output of its DSAR tool for Diagnostic Data, to make the events more comparable with intercepted network traffic. Publish a list of telemetry endpoints and their function, including an explanation about the specific endpoint for the exceptional OneDrive events that may contain readable usernames.

- Organise an independent verification of the explanation why the DSAR tool provides very limited access to *Required Service Data*: that the data are no longer stored as personal data, or were not collected as personal data.

- Make sure that no traffic is sent to third parties when the admin has disabled the Controller Connected Experiences. By the end of Q2 2022 all traffic to Bing should be removed from SharePoint Online when the organisation has disabled the Controller Connected Experiences. Microsoft must still take action to prevent any traffic to Cloudflare on Microsoft support pages that are accessed from links in Teams settings on the different platforms.

- Disable Teams Analytics & reports by default, and only enable the functionality if an admin so chooses, in order to comply with art. 25 GDPR. When an admin does not disable, and chooses to pseudonymise the data, inform about the consequences for the raw data held by Microsoft.

17.1.2 Measures government organisations and universities must take to mitigate the risks

Based on this DPIA, and repeating some recommendations following from earlier DPIAs for SLM Rijk, government organisations and universities must take the following measures to mitigate high data protection risks.

- Accept the temporary risk of the transfer of the pseudonymised Telemetry Data while Microsoft is building its EU Data Boundary. Do not exchange highly sensitive or special categories of personal data through Teams unless it is a public meeting.

- Enable E2EE in Teams for 1-on-1 conversations

- Enable E2EE in Teams for all meetings and chats as soon as Microsoft makes this available

- Consider the use of pseudonyms in the Azure AD for employees whose work identity must remain confidential. Use pseudonyms when the Azure AD is used for Single Sign On with external suppliers for employees whose work identity must remain confidential.

- Create a Teams and OneDrive privacy policy for internal users and guest users, establish a policy for the sharing of files and images. Make employees and guest users accept these rules through Terms & Conditions imposed by Azure AD.

- Use Double Key Encryption for documents with sensitive and special categories of data stored in SharePoint/OneDrive (including Teams recordings). Use Customer Key and Customer Lockbox for other stored personal data.

- Do not use SMS for authentication to prevent the transmission of unencrypted cell phone numbers. Instead, use the Authenticator app or a hardware token.

- Regularly use the Data Viewer Tool when and where available, and compare the results with Microsoft's public documentation.

- Use Microsoft's DSAR tool to obtain access to diagnostic data, and compare with an occasional network traffic analysis.

- Support a specific audit by SLM Rijk on Microsoft's collection and use of the *Required Service Data*.

- Disable the Additional Optional Connected Experiences in Office365.

- Disable access to third party applications in the app store in Teams.

- Warn end users not to insert images into SharePoint via the built-in Bing search engine for the next six months.

- Disable most of the functions in Teams Analytics & reports, and turn on the pseudonymisation option: do not enable Viva Advanced Insights.

- Create a policy to prevent use of Teams Analytics & reports as an employee monitoring tool. Conduct a DPIA prior to use of these analytic tools, certainly when used in combination with another Microsoft Windows & Office Analytical services.

- Set the telemetry collection in installed applications to the lowest "Neither" level.

- Set telemetry collection in Windows to the lowest "security" level.

- Disclose retention period policies and enforce compliance, delete outdated data (to mitigate the risks of access from the U.S.A.)

- Establish policies to prevent file names and file paths from containing personal data.

- Inform employees about their access possibilities via the Data Viewer tool, or by filing a DSAR with the admin of their organisation.

Conclusions

Since June 2019, as a result of the negotiations with SLM Rijk and SURF, Microsoft has implemented many legal, technical and organisational measures to mitigate the risks for data subjects when processing personal data by using Teams, OneDrive, SharePoint and the Azure AD. In reply to the initial findings of this DPIA, Microsoft has committed to improve some shortcomings, and has provided important assurances about its data processing.

However, in view of the Schrems-II ruling and the technical findings described in this report, Microsoft has to make more adjustments and improvements to mitigate the remaining high risk and the six identified low risks. Microsoft should commit to a clear deadline for the application of E2EE to all Teams exchanges., Additionally, Microsoft should become more transparent about the contents of *Required Service Data*, and provide its customers with independent verification of its compliance with the agreed purpose limitation and retention periods for these specific Telemetry Data. Microsoft should provide functioning Diagnostic Data Viewer tools for OneDrive on Windows and MacOS. Finally, Microsoft should comply with the requirement of data protection by default, and enable administrators to opt-in to any new analytics services, based on clear information about the data processing impact.

If government organisations and universities implement all recommended measures, there are no known high risks for the data processing.

Caveat. It is uncertain how the transfer risks will be assessed by the national data protection authorities, in their joint investigation into the use of cloud services by public sector organisations. The results are expected by the end of 2022. For this DPIA the transfer risks have been rigorously assessed, including a separate DTIA. If necessary, this DPIA and DTIA will be updated in 2023.

If the EDPB were to assess the risk of the data transfers as much higher, even after Microsoft has completed its EU Data Boundary, organisations in the Netherlands would in fact no longer be able to use the services of U.S. providers, and the consequences would be much greater than just the use of these Microsoft services.

APPENDIX 1

Separate document with technical analysis