Ministerie van Justitie en Veiligheid

DPIA Office 365 for the Web and mobile Office apps (March 2020)

Data protection impact assessment on the processing of diagnostic data

Version 1.1

Date	30 June 2020
Status	PUBLIC

Colophon

DPIA by	**Ministry of Justice and Security** **Strategic Vendor Management Microsoft** **(SLM Microsoft Rijk)** Turfmarkt 147 2511 DP The Hague PO Box 20301 2500 EH The Hague www.rijksoverheid.nl/jenv
Contact	Paul van den Berg E p.j.van.den.berg@minjenv.nl T 070 370 79 11
Project name	**DPIA report** diagnostic data processing in Microsoft Office 365 for the Web and mobile Office apps (report delivered March 2020, Update June 2020)
Appendix	Overview telemetry data observed in iOS and Office for the Web apps
Authors	**Privacy Company** Sjoera Nas and Floor Terra, senior advisors, with the help of work student Lotte aan de Stegge www.privacycompany.eu

CONTENTS

Figures and tables

Summary

The Microsoft Office 365 Enterprise license includes the use of three different versions of the Office 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, previously known as Office Online). This Data Protection Impact Assessment (DPIA) is a repeated assessment of the use of the last two versions of the software: Office for the Web and the mobile Office apps. The Dutch government's department managing strategic vendor relations with Microsoft (SLM Microsoft Rijk) has published the earlier DPIA on 23 July 2019.

This DPIA contains outcomes with respect to diagnostic data processing in Office for the Web and the mobile Office apps as at 31 March 2020. Since then, SLM Microsoft Rijk and Microsoft agreed upon measures to mitigate the six high data protection risks set out in the table below, as further described in the paragraph 'Mitigating measures Microsoft' of this summary and in Section 17.3 of this report. Once these measures have been implemented by Microsoft, and provided that government administrators apply the recommended measures in this DPIA, the high data protection risks for data subjects related to the collection of data about the use of Office for the Web and the mobile Office apps identified in this DPIA will be mitigated.

Outcome: six high data protection risks
The outcome of this DPIA is that there are six high data protection risks and three low data protection risks in spite of the contractual, legal and organisational measures that Microsoft has taken in the spring of 2019, and since the fall of 2019 to mitigate the data protection risks. These high risks are due to the following seven circumstances:

1. When using Office for the Web, Microsoft sends personal data to two American companies that are not processors: Optimizely and Giphy. From mobile Office apps, Microsoft sends traffic to six companies, of which four are not processors.
2. Microsoft behaves as independent data controller for the processing of telemetry data about the use of the mobile Office apps and the processing of personal data in connection with the Controller Connected Experiences in the mobile Office apps and Office for the Web. Microsoft may process personal data from and about the use of the use of these services for all 17 purposes mentioned in its general privacy statement.
3. Some telemetry events from Office for the Web contain content data, such as file-, pad- and usernames. It is not clear whether Microsoft is processor for these telemetry events.
4. Administrators are not able to minimise the telemetry level in the Office for the Web services. The new central telemetry choice for the mobile Office apps has not yet been created for the Teams, Outlook and OneDrive mobile Office apps on iOS and Android.
5. The possibility to centrally turn off the Controller Connected Experiences in Office for the Web and the mobile Office apps does not yet work in the OneDrive, Outlook and Teams apps on iOS and Android and not in the Teams and OneDrive browser versions of Office for the Web.
6. Microsoft does not publish information about the telemetry that it collects via Office for the Web and the mobile Office apps. Microsoft has now made the Data Viewer Tool suitable for decoding events from three mobile Office apps

on iOS and Android, namely Word, PowerPoint and Excel, but not for the Outlook, Teams and OneDrive apps.

7. Microsoft, when acting as controller, has not given access to the personal data that it processes via the mobile Office apps, the Controller Connected Experiences and the telemetry of Office for the Web.

The high risks and the possible countermeasures of Microsoft and of government organisations are listed below in a table.

Umbrella DPIA versus individual DPIAs

This DPIA was conducted by SLM Microsoft Rijk, the central negotiator for Microsoft products and services for Dutch central government organisations. However, the individual government organisations buy the licenses and determine the settings and scope of the processing by Microsoft. Therefore, this general DPIA can help the different government organisations with the DPIAs they must conduct, but this document does not replace the specific risk assessments the different government organisations 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.

Scope: diagnostic data, not content or functional data

This report addresses the data protection risks of the storing by Microsoft of data about the use of the five most commonly used applications (Word, PowerPoint, Outlook, Excel and Teams) in Office for the Web and the mobile Office apps, in combination with the use of Connected Experiences and the cloud services SharePoint, OneDrive for Business, Exchange Online and the Azure Active Directory. These metadata (about the use of the services and software) are called 'diagnostic data' in this report.

Technically, Microsoft Corporation collects diagnostic data in different ways, via system-generated event logs on its own cloud servers and via the telemetry client in the mobile Office apps and -since recently- also via Office for the Web. Similar to the telemetry client in Windows 10 and 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. The fact that Microsoft now also collects data via telemetry events via Office for the Web is new compared to the Office for the Web version that was checked in the previous (public) DPIA.

The diagnostic data are different from the data that users provide to Microsoft such as content data, and they are also different from the functional data that Microsoft has to temporarily process to allow users to connect to the internet and use Microsoft's online services.

Technical analysis personal data

The technical investigation of the data processing via Office for the Web, the Connected Cloud Services and the mobile Office apps was conducted by running a large number of scripted scenarios and intercepting and analysing the outgoing traffic.

In order to verify what personal data Microsoft collects about the use of Office for the Web, access requests were filed via Microsoft's Data Subject Request tool for the two test accounts, and the audit log files were queried. In addition, formal access requests were submitted to Microsoft as data controller, as referred to in Article 15 of the GDPR,

for the personal data about the use of the mobile Office apps and the Controller Connected Experiences. Microsoft did not provide the requested access.

Contents telemetry traffic
The study shows that Microsoft **collects limited data about the individual use of Office for the Web and the mobile Office apps via the telemetry events (as opposed to the telemetry flow from Office 365 ProPlus).** Privacy Company has not seen any content data in the telemetry events from the mobile Office apps, as far as they were readable. However, file-, path- and usernames were found in telemetry events from PowerPoint and Word in Office for the Web.

Contents log files cloud servers
The automated access requests (DSARs) show that Microsoft processes directly identifiable personal data in its diagnostic data about the use of Office for the Web applications in combination with its Connected Cloud Services. These data contain the username and email address in combination with the time (accurate to the second) at which individual employees have performed activities in the applications. In these log files Microsoft also collects content data on the titles, pathnames, subjects of files or emails, all email addresses of direct and indirect addressees (to, cc and bcc), whether there were attachments to the email and the size of the files in KB.

Outgoing traffic to third parties
The intercepted traffic shows that Microsoft sends traffic from Office for the Web and from the mobile Office apps to respectively two and six third parties. Microsoft has a processor agreement with two of these parties (Akamai and UserVoice).

Microsoft transfers personal data from Office for the Web to two third parties: Optimizely and Giphy. Traffic goes to Optimizely when a user wants to log in to OneDrive via Office for the Web and to Giphy when a user wants to insert an image in Teams. Giphy and Optimizely are missing from the exhaustive list of subprocessors that Microsoft engages for the Core Online Services. Microsoft does not publish any information about the processing of personal data by these parties. System administrators can disable traffic to Giphy with a specific group policy, but this possibility does not exist for the traffic to Optimizely.

Microsoft sends personal data from four mobile Office apps (OneDrive, Outlook, Word and Teams) to five companies in the United States and one company in Germany without users knowing, and without information about the purposes of this processing. The five U.S. companies are: Akamai, Cloudflare, Giphy, Helpshift and UserVoice. Akamai and Cloudflare are content delivery networks, offering local copies of content. Cloudflare also provides security services, such as checking blacklists of IP addresses of known hackers and spammers. Helpshift provides in-app tools to improve customer service, UserVoice specialises in digital customer research. The German company Adjust GmbH specializes in measuring the reach of, and combatting fraud with, mobile ads.

Although the information from the mobile Office apps that a unique user worked with a Microsoft Office application at a specific time does not in itself reveal personal data of a sensitive nature, the information is forwarded to companies in Germany and the United States of which it is not clear to what extent they are bound by Microsoft's privacy guarantees. The companies' privacy statements show that most companies use the personal data collected for their own analysis purposes, and in many cases (Cloudflare, Giphy, Optimizely, UserVoice) also for displaying personalised advertisements.

Although Microsoft has processing agreements with Akamai and UserVoice, when using UserVoice, Microsoft does refer to the company's own privacy policy. According to that statement, UserVoice also processes the data that it receives as a processor for its own purposes as a controller. UserVoice can combine the diagnostic data from the Outlook and Teams apps with questions/complaints that users publish in the UserVoice discussion forums. UserVoice thus actually creates profiles of users of these apps.

Purposes, roles and legal grounds
The privacy amendment negotiated by SLM Microsoft Rijk in May 2019 for the Dutch government 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 where 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 Office for the Web, the Processor Connected Experiences and the Connected Cloud Services SharePoint Online, OneDrive for Business, Exchange Online and the Azure AD. However, this DPIA shows that Microsoft does not correctly apply its role as a processor in respect of Office for the Web. Microsoft did not implement telemetry control settings for Office for the Web and sends personal data to third parties that are not authorised subprocessors. In those instances, Microsoft factually acts as a joint controller together with the relevant government organisation.

The right to use the mobile Office apps with a work or school account is granted in Microsoft's Online Service Terms. As a result, the data protection terms of Online Service Terms, the Data Protection Addendum and the privacy amendment apply to the processing of all personal data received, collected, generated or derived through the use of the mobile Office apps with a work or school account. This includes personal data in diagnostic data (including telemetry). It makes no difference whether the diagnostic data relates to the performance of the mobile Office application on the device or the use of the Office application itself. All personal data associated with organisational credentials falls within the scope of the privacy amendment. This means that that Microsoft may only act as a processor, except for the Controller Connected Experiences and certain purposes for which it has a legitimate business interest. Microsoft may only send personal data to third parties if they are approved as subprocessors under the privacy amendment or in connection with Controller Connected Experiences that are not disabled by the relevant government organisation.

In its response to the DPIA findings of 6 March 2020, Microsoft states that for data processing occurring under organisational credentials *relative to Online Services* accessible within the mobile Office apps, Microsoft is a processor and acting in accordance with processing instructions. This answer and the DPIA findings show that Microsoft somehow acts under the assumption that it has the discretion to process personal data obtained through use of a mobile Office app with organisational credentials as a controller for purposes that have not been authorised by the government organisation, simply by labelling such processing *not* relative to Online Services. Microsoft takes the view that such use is governed by a direct license

agreement with the end user, and is subject to Microsoft's own privacy statement as Microsoft is an (independent) controller. This is wrong. Because Microsoft may only act as a processor, any functionality or processing outside of the customers instructions must be authorised by the controller, which is the government organisation and not Microsoft. There is no room for Microsoft to determine additional purposes or to offer additional functionality to end users outside of the government organisation's documented instructions. The only exceptions are the Controller Connected Experiences that have not been disabled by the government organisation, processing for Microsoft's own legitimate business purposes (e.g. invoicing) and disclosures to authorities when Microsoft is legally prohibited from redirecting the order to the customer.

As a result of the incorrect application of the scope of the Online Services, Microsoft is a controller for the collection of diagnostic data for the mobile Office apps. As government organisations are also controllers, this means that Microsoft is a joint controller with the government. This means that Microsoft and the government have an obligation to comply to art. 26 GDPR (which in practice should lead to a joint-controller agreement).

The DPIA findings show that Microsoft, contrary to the customer's instructions, sends personal data to third parties that are neither authorised as subprocessors under the privacy amendment nor duly qualified as Controller Connected Experiences. Microsoft claims that these parties offer functionality that fall outside of the scope of the Online Services, and can therefore be offered by Microsoft as a controller. However, as set out above, this is not correct. If Microsoft does not act as a processor and engages or offers the service of a third party, Microsoft may become a joint controller with the government entity and/or the third party.

Microsoft considers itself a controller with respect to diagnostic data about the use of the mobile Office apps and therefore processes personal data under its privacy statement. The seventeen purposes mentioned in the privacy statement for which Microsoft allows itself to process the data are too broad and often too undefined. There is no legal ground for most of these purposes.

Microsoft's processing role for the Connected Experiences differs depending on the type of Connected Experience. Since May 2019, Microsoft distinguishes between Connected Experiences for which it is the data controller (the Additional Optional Connected Experiences) and the Connected Experiences for which it is processor (Connected Experiences not included in the list of Additional Optional Connected Experiences, referred to in this report as Processor Connected Experiences). Since then, Microsoft has been processor for most commonly used Connected Experiences such as the Editor (spelling and grammar checker) and the translation module. However, Microsoft's information about the different types of Connected Experiences is (still) not clear and not complete. According to the privacy amendment with the Dutch government, Microsoft is the controller for the 14 listed Controller Connected Experiences. However, not all of these services are available in the mobile Office apps and in Office for the Web, while there are new / other Connected Experiences for which Microsoft apparently also acts as controller.

As mentioned above, the government organisations are currently joint controllers with Microsoft for the investigated processing of the diagnostic data via the mobile Office apps, the use of the Controller Connected Experiences that cannot be disabled via the Additional Optional Connected Experiences and (in connection with the transfer of personal data) for the processing by third parties of personal data about the use of Teams and OneDrive via Office for the Web. As a result, the government organisations

are accountable for the risks that data subjects run of unlawful processing of their personal data.

High risks and mitigating measures
At the date of completion of the DPIA on 31 March 2020, the processing of diagnostic data about the use of Office for the Web and the mobile Office apps in the Enterprise environment, leads to **six high data protection risks for data subjects**.

Six high risks	Measures government organisations	Measures Microsoft
Lack of purpose limitation for the diagnostic data from mobile Office apps and Office for the Web	Block access to the Outlook, Word, Teams and OneDrive apps from the work accounts on iOS and Android	Only act as processor for the mobile Office apps (except for the Controller Connected Experiences and Microsoft's own legitimate business interests), not as controller, and process the data only for the three authorised purposes
	Discourage log-in to OneDrive via Office for the Web	Only use authorised subprocessors with the Online Services. If Microsoft wishes to engage subprocessors, they must be approved in accordance with the privacy amendment with the Dutch government
	Block traffic from the apps to Giphy, Adjust, Helpshift and UserVoice with group policies	
	Establish policies to prevent file names and path names from containing personal data	Stop sending personal data to third parties unless the third party is an authorised subprocessor or the traffic is approved in connection with an enabled Controller Connected Experience or enabled Add-in and ensure that all Controller Connected Experiences can be centrally turned off by administrators
Lack of transparency diagnostic data Office for the Web, the mobile Office apps, Connected Experiences and Connected Cloud Services	Inform employees of the possibilities for Data Subject Access Requests and access to the audit logs	Publish exhaustive and comprehensible documentation about the processing of diagnostic data from the mobile Office apps, Office for the Web, all Connected Experiences and the Connected Cloud Services
	The administrators must regularly use the Data Viewer Tool for the mobile Word, PowerPoint and Excel apps	Make the Data Viewer Tool available for traffic from the Outlook, Teams and OneDrive mobile Office apps and in a similar way give

	As soon as Microsoft makes a tool available to inspect the telemetry from Office for the Web and the other mobile Office apps, use this tool regularly as well	insight in the telemetry from Office for the Web
	Disclose and enforce retention policy / clean up obsolete data	
Lack of control: telemetry level Office for the Web and the mobile Outlook, Teams and OneDrive apps	Retest the new versions of the mobile OneDrive, Outlook and Teams apps	Only act as processor for the mobile Office apps, process the data only for the three authorised purposes
	Recommend users to use the newest versions of these apps when the privacy risks have been mitigated	Implement telemetry choice controls for administrators for the mobile OneDrive, Outlook and Teams apps
	As soon as it is possible: set the lowest telemetry level in mobile Office apps and Office for the Web	Implement the central privacy control for telemetry in Office for the Web
Lack of control: transfer of personal data from Office for the Web to third parties	Discourage log-in to OneDrive via Office for the Web and centrally block traffic to Giphy with group policy	Do not embed services in the Online Services that transfer personal data to third parties, unless the third party is an authorised subprocessor or (part of) an enabled Controller Connected Experience
Lack of control: transfer of personal data from mobile Office apps to third parties	Block access to the mobile OneDrive, Outlook, Teams and Word apps	Do not transfer personal data via the mobile Office apps to third parties if they are not authorised subprocessors
	Block traffic from the mobile Office apps to Giphy, Adjust, Helpshift and UserVoice	
No access for data subjects	Block access to the mobile Outlook, Word, Teams and OneDrive apps	Honour data subject access rights, preferably by expanding the current DSAR tool to include all data collected through the Connected Experiences, Azure AD and mobile Office apps
	Turn off all Controller Connected Experiences	

Microsoft measures

This DPIA was conducted between January and March 2020 and contains outcomes with respect to diagnostic data processing in Office for the Web and the mobile Office apps. The initial version of this report was completed on 31 March 2020. SLM Microsoft Rijk provided Microsoft with the DPIA findings upon completion of this DPIA. Between April and June 2020, SLM Microsoft Rijk and Microsoft discussed measures to mitigate

the six high data protection risks. Microsoft will have mitigated risks 1, 4 and 5 before the end of the summer of 2020; other risks before the end of 2020.

Once these measures have been implemented by Microsoft, and provided that **government administrators apply the recommended measures in this DPIA, the high data protection risks for data subjects related to the collection of data about the use of Office for the Web and the mobile Office apps identified in this DPIA will be mitigated.** SLM Microsoft Rijk will publish an update about the progress of the implementation of the measures early in 2021.

In May 2019, the Dutch government obtained effective audit rights, and will have an independent auditor perform an annual audit to verify compliance with the privacy amendment. A summary of the findings will be published by SLM Microsoft Rijk.

The table below contains an overview of the measures that will mitigate the high risks. section 17 of this report contains further details about these measures and the remaining low risks.

Overview of measures to mitigate high risks

No.	High risks	Agreed measures Microsoft
1	Lack of purpose limitation for the diagnostic data from mobile Office apps and Office for the Web	Only act as processor for the mobile Office apps (except for the Controller Connected Experiences and Microsoft's legitimate business purposes), not as controller, and process the data only for the three authorised purposes
		Only use authorised subprocessors with the Online Services. If Microsoft wishes to engage subprocessors, they will be approved in accordance with the privacy amendment with the Dutch government
		Microsoft will stop sending personal data to third parties unless the third party is an authorised subprocessor or the traffic is approved in connection with an enabled Controller Connected Experience or enabled Add-in
		Microsoft will ensure that all Controller Connected Experiences can be centrally turned off by administrators
2	Lack of transparency diagnostic data Office for the Web, the mobile Office apps, Connected Experiences and Connected Cloud Services	Publish exhaustive and comprehensible documentation about the processing of diagnostic data from the mobile Office apps, Office for the Web, all Connected Experiences and the Connected Cloud Services
		Make data viewing capabilities available for traffic from the Outlook, Teams and OneDrive mobile Office apps
3	Lack of control: telemetry level Office for the Web in the mobile Outlook, Teams and OneDrive apps	Only act as processor for the mobile Office apps, process the data only for the three authorised purposes
		Implement telemetry choice controls for administrators for the mobile OneDrive, Outlook and Teams apps

		Implement technical measures to ensure that diagnostic data collection with respect to Office for the Web will be limited to the minimum necessary data
4	Lack of control: transfer of personal data from Office for the Web to third parties	No embedding of services in the Online Services that transfer personal data to third parties via Office for the Web, unless the third party is an authorised subprocessor or (part of) and enabled Controller Connected Experience
		Microsoft will ensure that the third parties identified in this DPIA will either be removed from the service, authorised as a subprocessor, or become (part of) a Controller Connected Experience
5	Lack of control: transfer of personal data from mobile Office apps to third parties	No embedding of services in the Online Services that transfer personal data via the mobile Office apps to third parties if they are not authorised subprocessors or (part of) and enabled Controller Connected Experience
		Microsoft will ensure that the third parties identified in this DPIA will either be removed from the service, authorised as a subprocessor, or become (part of) a Controller Connected Experience
6	No access for data subjects	Microsoft will honour data subject access rights where it is a processor by expanding the current DSAR tool to include all data collected through the Connected Experiences, Azure AD and mobile Office apps
		Microsoft will honour data subject access requests for the personal data Microsoft collects as data controller

Government organisations should implement the following measures to mitigate the high risks.

1. Turn off the Controller Connected Experiences.
2. Set the telemetry level of the mobile Office apps to the lowest level.
3. Administrators must regularly use the Data Viewer Tool to view the telemetry sent from the mobile Office apps.
4. Disclose and enforce retention policy / clean up outdated data due to risks of transfer to the US.
5. Retest new versions of the mobile Office apps / recommend users to install the latest versions as soon as the privacy risks have been mitigated.
6. When using the Connected Cloud Services (OneDrive, SharePoint, Exchange Online), establish policies to prevent file names and file paths from containing personal data.
7. Inform employees about the access possibilities via DSR and audit logs.

Conclusions

Since June 2019, as a result of the negotiations with SLM Microsoft Rijk, Microsoft implemented a number of legal, technical and organisational measures to mitigate the risks for data subjects when processing personal data by using Office for the Web and the mobile Office apps.

Despite these improvements, this DPIA shows that the use of Office for the Web and the mobile Office apps in combination with the Connected Experiences and the Connected Cloud Services still leads to six high and three low data protection risks for data subjects. Some of these risks are new, for example because Microsoft only recently started collecting telemetry events via Office for the Web, or because Microsoft transfers traffic via the apps and Office for the Web to third parties that are not subprocessors of Microsoft. Other risks are related to the fact that some improvement measures have not yet been implemented effectively. In particular Outlook, Teams and OneDrive are lagging behind.

In order to eliminate the high risks, Microsoft may only act as data processor for all the services included in the Office 365 licence, including the mobile Office apps, and therefore processes the data only for the authorised three necessary purposes. This also means that Microsoft should stop sending traffic to third parties if those recipients are not bound by a subprocessor agreement to the three purposes for which Microsoft is allowed to process the personal data from Dutch government organisations. Microsoft must also publish up to date, exhaustive and comprehensible information about the telemetry data it collects via Office for the Web and the mobile Office apps, and the diagnostic data it collects via the cloud logs, the Azure AD, and the Connected Experiences. Last but not least, Microsoft should provide a tool to decipher the telemetry events from Office for the Web and all the mobile Office apps.

Following completion of this DPIA, SLM Microsoft Rijk and Microsoft agreed upon measures to mitigate the high risks. Some measures will be implemented before the end of the summer of 2020, others ultimately by the end of 2020. **Once implementation has been successfully completed, and assuming government organisations follow the recommendations set out in in this report, all high risks identified in this DPIA will be mitigated.**

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 Microsoft Strategic Vendor Management office (SLM Microsoft Rijk[1]) of 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]

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.[3]

[1] SLM is the abbreviation of the Dutch words Strategisch Leveranciersmanagement Microsoft.
[2] DPIA Microsoft Office 365 Online and Mobile SLM Microsoft 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] *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017). For an explanation and examples (in Dutch) see: https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia.

Umbrella DPIA versus individual DPIAs

The Microsoft Office 365 software is used by approximately 300.000 employees and workers in the Dutch ministries, parliament, the High Councils of state, the advisory commissions, the police, the fire department and the judiciary, as well as the independent administrative authorities.[4] The Microsoft Office software is not new, but in the volume licensing agreements, Microsoft releases new versions with new functionalities twice per year. 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 in the Netherlands to conduct a DPIA based on the criteria published by the Dutch data protection authority.[5]

In GDPR terms SLM Microsoft Rijk **is not the data controller** for the processing of diagnostic data via the use of the Office software. The data controller is the individual government organisation that offers the use of the Office software to its employees. However, as central negotiator with Microsoft, it has 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 Microsoft Rijk commissions umbrella DPIAs to assist the government 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 government 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 Microsoft Rijk

Simultaneously with this DPIA about Office for the Web and the mobile Office apps, SLM Microsoft Rijk also publishes a DPIA on the risks of the processing of diagnostic data via Microsoft Intune and the Company Portal app.[6]

The role of SLM Microsoft Rijk is not limited to Microsoft Office. As representative of all the procuring government organisations, SLM Microsoft Rijk assesses the risks for all Microsoft products and services that are commonly used by government organisations, such as Windows, Office, Dynamics and Azure and approaches the risk mitigating measures with a holistic view. Microsoft has been working constructively with SLM Microsoft Rijk during the review of the risks of the use of these products.

As part of its ongoing commitment to ensure GDPR compliance, SLM Microsoft Rijk regularly commissions new DPIAs on new versions of Windows 10 and Office 365, to

[4] Source: Microsoft Business and Services Agreement, Amendment ID CTM, May 2017, last amended 10 May 2019.

[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.

[6] See the website of SLM Microsoft Rijk (Department of Justice Dutch government), URL: https://www.rijksoverheid.nl/documenten/publicaties/2018/11/12/strategisch-leveranciersmanagement-microsoft-rijk-slm-microsoft.

guarantee the rights of data subjects on ongoing basis. New DPIAs can be necessary to examine the risks of changes in the technology and processing methods, to take account of modifications of the applicable laws and/or relevant jurisprudence, and to assess changes in the contractual agreement with Microsoft.

In November 2018 SLM Microsoft Rijk published a first DPIA on the data protection risks of the autumn 2018 version of Office 365 ProPlus, version 1708.[7] The report was published on the Dutch government website with an update on the negotiations between the Dutch central government and Microsoft about the GDPR compliance.[8]

Simultaneously with the DPIAs on Office 365, SLM Microsoft Rijk also commissioned a renewed DPIA on Windows 10 Enterprise. This new assessment on the data protection risks of Windows 10 Enterprise version 1809 and 1903 recommends to update to the 1903 version or later, and concludes that there are no high data protection risks when the telemetry level is set to Security, and admins prevent users from syncing their activities via the Windows 10 Timeline.

SLM Microsoft Rijk also commissioned DPIAs on the data processing risks of using Microsoft's Azure cloud services and Microsoft Dynamics.

The DPIA reports have been written by the Dutch privacy consultancy firm Privacy Company.[9]

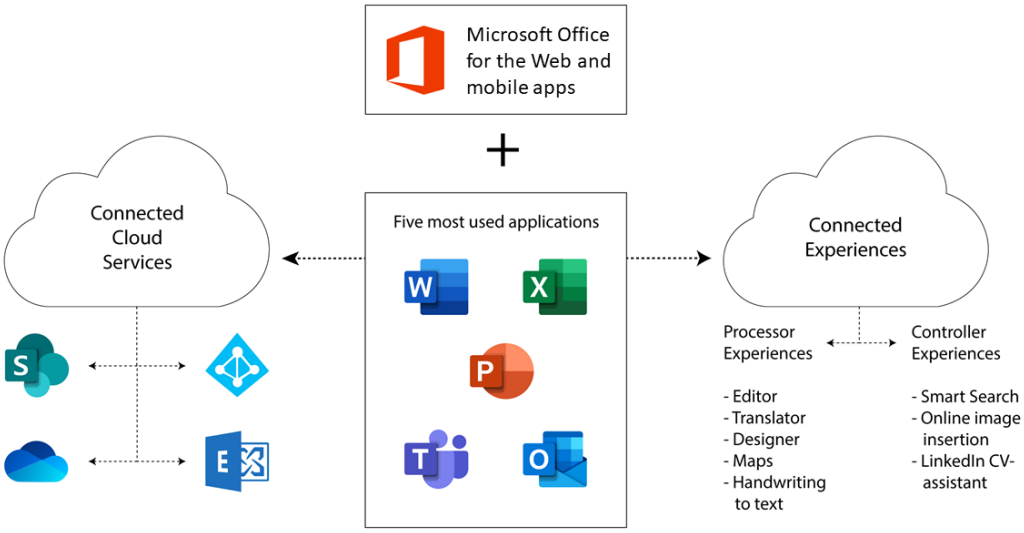
Scope of this DPIA: Office for the Web and mobile Office apps

This DPIA addresses the risks of data processing on the individual use of Office for the Web and the mobile Office applications, which are available for iOS and Android.

This report charts the risks of data processing via the five most commonly used applications expected: Word, PowerPoint, Outlook, Excel and Teams in combination with the use of additional online services such as the spell checker (Connected Experiences), the cloud storage services SharePoint Online/OneDrive for Business, the cloud identity service (Azure Active Directory) and the online mail server (Exchange Online). These four types of cloud services are referred to in this report as 'the Connected Cloud Services'.

[7] This first Office ProPlus DPIA report also assessed the risks of Office 2016 ProPlus, and was published on 7 November 2018, with an update on the negotiations between the Dutch central government and Microsoft about the GDPR compliance. URL: https://www.rijksoverheid.nl/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office.
[8] Ibid.
[9] https://www.privacycompany.eu/

Figure 1: Scope of this DPIA report



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 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.

This report does not assess the risks of storing content data on Microsofts cloud servers, i.e. the documents, files and emails. The general risks of storing data on cloud servers fall outside the scope of this report.

Methodology

Privacy Company applied three different investigation methods:

1. the interception and decoding of data traffic from the two iOS and Android smartphones;
2. accessing the audit logs and using Microsofts Data Subject Access Request tool for admins after having used Office for the Web and the Connected Cloud Services;
3. filing an access request directly with Microsoft as data controller for data collected from the mobile Office apps and the Controller Connected Experiences.

Specific test scenarios were executed in the five most commonly used apps (Word, Outlook, Excel, PowerPoint and Teams). Additional online services were used in each of the apps, such as the Editor (spelling and grammar checker), Translator (translation module) and inserting an image from the Internet (Insert Online Pictures). Microsoft calls these extra services 'Connected Experiences' since May 2019. The scenarios have been developed to best reproduce the everyday actions of users. The scenarios were executed on 20, 21 and 28 January 2020 (Teams).

The telemetry traffic from the apps and via the browser is encoded in an undocumented format. As a result, it is not easy to analyse the content of the events. The structure of the events is not entirely clear. Pieces of text are easy to recognise, but some parts of a event are not saved as readable text and are therefore not easy to understand. Privacy Company tested for a limited period of time. As a result, Privacy Company did not detect all types of telemetry events.

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 network termination points found and the captured telemetry events are recorded in Appendix 1 to this report.

Settings in the test environment
The level of telemetry events was set to the lowest level 'Neither'. All four types of Connected Experiences were blocked. These four types are: the two types of Connected Experiences that analyse or download content, other Connected Experiences and the specific set of Additional Optional Connected Experiences for which Microsoft is controller. These are services related to the use of Bing, LinkedIn and the Office Store. In the Office for the Web environment, Microsoft only offers the possibility to block the latter group of Controller Connected Experiences, not the first three types. In the test environment access to *all* Connected Experiences was blocked. Privacy Company tested as many available Connected Experiences as possible in Office for the Web. If a certain Connected Experience was not available, this is indicated in Appendix 2.

Data subject access requests
Microsoft processes usage data on its own cloud servers about the use of the Connected Experiences, Office for the Web and the Connected Cloud Services SharePoint Online/OneDrive for Business, Exchange Online 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, (automated) data subject access requests were filed for the two test accounts by the administrator in the dedicated Data Subject Request tool Microsoft offers to administrators for this purpose. Additionally, the audit log files were inspected with detailed information about the activities performed by the investigators.

Microsoft does not display update information or version history for Office for the Web. Privacy Company tested the version of Office for the Web that was available on 20 January 2020 through the Office 365 license and performed the tests with a Chrome Browser, version 79.0.3945.117 (Official Build) (64-bit) on a Macbook pro, with OS version macOS Catalina version 10.15.0.

Interception of the telemetry traffic
On iOS, Privacy Company reviewed the following mobile versions of the Office apps on an iPhone 7 running iOS version 12.3.1: Excel/2.33.20010900, OneDrive/11.15.8, PowerPoint/2.33.20010900, Microsoft Office Word/2.33.109, Outlook/3623017 and Teams version 2.0.1.

On Android, Privacy Company investigated the following mobile versions of the Office apps on a Pixel 3 XL, with Android operating system version 10, security patch level 1 January 2020. The following versions of the apps have been tested: Microsoft OneDrive 5.46, Microsoft Excel 16.0.12325, Microsoft Office Word 16.0.12325,

Microsoft PowerPoint 16.0.12325, Microsoft Outlook 4.1.9 and Microsoft Teams version 1416/1.0.0.2020012501.

Privacy Company intercepted the outgoing telemetry data from the two smartphones with Mitmproxy version 4.0.4 (software that makes it possible to inspect the content of traffic with and without TLS encryption).

The Mitmproxy was used as follows:
Configure the laptop to use the proxy
Start the Mitmproxy
Launch the specific mobile application
Log in with an Office365 account as needed
Run the scripted scenario. Make screenshots of each step.
Once the script is fully executed, stop the Mitmproxy.

Privacy Company saved the log files and compared the network endpoints with the limited public information Microsoft publishes about them.[10]

There are two telemetry endpoints in the network traffic: browser.pipe.aria.microsoft.com and mobile.pipe.aria.microsoft.com.
The data sent to the second endpoint, mobile.pipe.aria.microsoft.com, was encrypted in an undocumented binary format. The raw data were searched in a structured way with specific search scripts, partly based on the content of the test scenarios.

Response Microsoft

On 6 March 2020, a representative of Microsoft gave written comments on the technical findings. Microsoft provided arguments and reasons for the observed outgoing traffic to third parties, and replied to the observations about missing controls for system administrators. Microsoft's specific answers are quoted further on in the report, in the relevant Sections.

Outline

This assessment follows the structure of the *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017).[11] 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 by Office for the Web and the mobile Office apps 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 Microsoft Rijk have already been processed.
Part B provides an assessment (by Privacy Company, with input from the Ministry of Justice and Security) of the lawfulness of the data processing. This analysis starts

[10] https://docs.microsoft.com/en-gb/office365/enterprise/urls-and-ip-address-ranges
[11] 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

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 in particular by the processing activities related to the collection of usage data from the Connected Experiences and the mobile Office apps.

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

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 the use of Office 365 for the Web and via the mobile Office apps. This 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 Office for the Web and the mobile Office apps, in combination with the Connected Experiences and the use of the Connected Cloud Services SharePoint Online, OneDrive for Business, the online mail server Exchange Online and the cloud authentication service Azure Active Directory. The data processing is tested via the five most widely used applications: Word, Word, PowerPoint, Outlook, Excel and Teams in combination with the use of Connected Experiences such as the Editor.

1.1 About Office for the Web, the mobile Office apps and the Connected Experiences

The Microsoft Office 365 software includes some of the most popular and widely used computer programs to help people send emails, write, calculate, present, chat, collaborate and organise work tasks. Given the general familiarity of the Office package, this report does not provide a separate explanation about the functionality of the various programs and services.

Office ProPlus, Office for the Web and mobile Office apps

The Office 365 software can be used in three ways. The software can be installed on the computers and laptops of data subjects (the ProPlus version, or the locally installed Office 2016 or Office 2019 software), but the software is also available in the form of online applications that run in a browser (Office for the Web), and as applications for mobile devices (the mobile Office apps) with Android or iOS as the operating system.

Office 365 account

If Dutch government employees want to use Office 365 for work purposes they must have an Office 365 work account and be assigned a license.[12] Office 365 Enterprise

[12] 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*

and Education accounts and their related licenses are registered in the Azure Active Directory.

Connected Experiences
The Office software and applications allow the use of a large number of Connected Experiences such as the Editor (spelling and grammar checker), the possibility to insert an image or a translation module. Before May 2019, Microsoft called these services 'Connected Services' or 'Micro services'.

Legally, Microsoft offers the Connected Experiences in two 'flavours': either included, where Microsoft acts as processor (Processor Connected Experience), or optional, where Microsoft acts as controller (Controller Connected Experience). In its public explanation, Microsoft distinguishes between four types of Connected Experiences, which partly overlap each other. Microsoft does not make a clear distinction in its documentation between the services for which it acts as controller and the services for which it acts as processor. Instead, Microsoft categorizes the Connected Experiences in four groups, namely:

1. services that analyse your content,
2. services that download online content,
3. other services
4. Additional Optional Connected Experiences.[13]

Services that fall into the group Additional Optional Connected Experiences are all 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 as a service uses search engine Bing or the social network LinkedIn.

As a result of the first public DPIA of SLM Microsoft Rijk, Microsoft implemented a major change in the Connected Experiences in May 2019, simultaneously with the launch of the new semi-annual version of the Office 365 ProPlus software. Microsoft's role for most Connected Experiences was shifted to that of processor.[14] This means that Microsoft processes the personal data from these services for the same (limited set of) purposes as its other Online Services. As a result of this reclassification, frequently used Connected Experiences such as the Editor and Translator should now qualify as Processor Connected Experiences and fall under the guarantees of the global privacy guarantees of Microsoft's Online Service Terms, the included Data Protection Addendum and the contractual amendment as agreed with SLM Microsoft Rijk. However, this DPIA shows that Microsoft has not yet fully and correctly implemented its roles as processor and controller for the Connected Experiences (see paragraph 16.2.3 and 16.2.3 of this report).

---

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

[13] 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

[14] Idem. Also see: Required service data for Office, 11 October 2019, URL: https://docs.microsoft.com/en-gb/DeployOffice/privacy/required-service-data Essential services events (Connected experiences), https://docs.microsoft.com/en-gb/DeployOffice/privacy/essential-services and Microsoft, Essential services for Office, 12 December 2019, URL: https://docs.microsoft.com/en-gb/DeployOffice/privacy/essential-services

Controller Connected Experiences

Microsoft publishes a list of 15 Additional Optional Connected Experiences that are available in combination with Office 365 ProPlus.[15] These are services that use, for example, search engine Bing or LinkedIn, or the Office Store. When using these services, Microsoft considers itself as (independent) controller for the processing of the data.

The privacy terms that SLM Microsoft Rijk negotiated with Microsoft in May 2019 list 14 services as Controller Connected Experiences. The contractual amendment acknowledges that this list is dynamic and subject to change, as Microsoft may add or remove Controller Connected Experiences, but only insofar as the service is duly included in the list of Additional Optional Connected Experiences on the Microsoft website.[16]

The list of Controller Connected Experiences included in the contractual amendment does not correspond with the available Controller Connected Experiences in the test environment in Office for the Web and the mobile Office apps. It was a puzzle to discover for which of the Connected Experiences that are currently available in the various tested applications in Office for the Web and in the mobile Office apps, Microsoft considers itself to be controller.

The table below lists the Additional Optional Connected Experiences available in the test environment (right column) and compares these to the Controller Connected Experiences included in the contractual amendment (left column).

Table 1: Available Additional Optional [Controller] Connected Experiences

Controller Connected Experiences contract amendment	**Test environment**
3D Maps	Not available
Researcher	Not available
Giving Feedback to Microsoft	Available as 'Feedback': available in Word, PowerPoint, Outlook, Excel and Teams in Office for the Web and in all tested mobile Office apps on iOS and Android
Smart Lookup	Smart searching via Bing: available in Word in Office for the Web and the mobile Office apps
Insert 3D Models	Insert 3D-images online: available in PowerPoint for the Web en in the mobile Office apps
Insert Online Pictures	Insert online images via Bing: available in Word, PowerPoint, Outlook, Teams (not available in Excel) for the Web and in the mobile Office apps
Map Chart	Not available
Resume Assistant	Not available

[15] Microsoft, Overzicht van optioneel verbonden functies in Office, 14 januari 2020, URL: https://docs.microsoft.com/nl-nl/deployoffice/privacy/optional-connected-experiences
[16] Microsoft, Overview of optional connected experiences in Office, 29 February 2020, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/optional-connected-experiences

Office Store	Office plugins – Store: available in Word, PowerPoint, Outlook for the Web
Weather Bar	Weather bar: available in Outlook for the Web and mobile Office app
Online Video	Embed an Online Video: available in PowerPoint for the Web and mobile Office apps
Suggest a Feature	Suggest a Feature: available in Word, PowerPoint, Outlook, Excel and Teams for the Web and in every Mobile Office app on iOS and Android
QuickStarter	Not available
Research	Not available
Not mentioned	Contact Support: added to Additional Optional Connected Experiences is March 2020, both for the Web and mobile Office apps
Not mentioned	Location Suggestion: available in Outlook for iOS and Android, added to Additional Optional Connected Experiences in March 2020

As set out in the table above, only 10 Additional Optional Connected Experiences should be available in the test environment. However, in addition to the Additional Optional Connected Experiences listed in the table, the Connected Experiences 'Vote for items' (only in Outlook for the Web, as Feedback functionality) and 'Cloud fonts' (available in Word and PowerPoint in Office for the Web and the mobile Office apps) were also available in the test environment. On the website specific to the service Cloud fonts, Microsoft explains that this is an Additional Optional Connected Experience.[17] However, this service is not included in the webpage with all Additional Optional Connected Experiences.[18]

In total, there were 12 Controller Connected Experiences available in the test environment.

The following Controller Connected Experiences are in any case **not available** in Office for the Web and the mobile Office apps: 3D Cards, Card Charts (also called 2D Cards), PowerPoint Quick Start, Researcher, Interesting calendars of sports teams or TV programs in Outlook for iOS and Android, the LinkedIn resume assistant (which is only available for English documents) and LinkedIn link with Microsoft account and, finally, enable Outlook Connector for social networks.

Since the end of May 2019, system administrators can choose to centrally disable the Additional Optional Connected Experiences in Office 365 ProPlus. Since autumn 2019 or January 2020 (depending on the chosen update regime) system administrators can also switch off the use of Additional Optional Connected Experiences in Office for the

[17] Microsoft, Cloud fonts in Office, 16 January 2020, URL: https://support.office.com/en-gb/article/cloud-fonts-in-office-f7b009fe-037f-45ed-a556-b5fe6ede6adb? The explanations show that this is a Controller Connected Experience. Microsoft writes: "*go to **File** > **Account**, select **Manage Settings** under **Account Privacy**, and turn on **Optional connected experiences**. Clearing the check box turns off cloud fonts and other online services from Microsoft.*"

[18] Microsoft, Overview of optional connected experiences in Office, 29 February 2020, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/optional-connected-experiences

Web and in some mobile Office apps. See the explanation and figures 8, 9 and 10 in section 3.1 of this report.

Processor Connected Experiences

From the investigation and from the various lists of Microsoft's Connected Experiences it seems as if there are 26 Processor Connected Experiences. The table below describes for what applications they are available, on the Web and/or as mobile Office app.

Table 2: Overview of the 25 available Processor Connected Experiences in Office for the Web and the mobile Office apps[19]

Name	Explanation and availability for the different platforms
Dictate	Available in Word, Excel and PowerPoint in Office for the Web applications. Dictate with your voice in Office For the Web.[20]
Editor (spelling and grammar checker)	Available in Word, Excel and PowerPoint in Office for the Web applications[21] and the mobile Word apps on iOS and Android.[22]
Insert data from image	Available in Excel on iOS and Android, not in Office for the Web[23]
Handwriting to text, Handwriting to form, Handwriting to mathematics	Only available in PowerPoint for iPad.[24]
Live-subtitles and captions	Available in PowerPoint for the Web. Present with realtime, automatic subtitles or captions.[25]
PowerPoint Designer	Available in PowerPoint for the Web and mobile PowerPoint apps on iOS and Android.

[19] The overview consists of all Connected Experiences published by Microsoft, minus the Controller Connected Experiences. Besides the services that analyse and download content, Microsoft also sums Connected Experiences under the heading of 'Other connected experiences', URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/connected-experiences.

[20] Microsoft, Dictate your documents, Web, URL: https://support.office.com/en-gb/article/dictate-your-documents-d4fd296e-8f15-4168-afec-1f95b13a6408

[21] There is no spelling checker available in Outlook for the Web. See: Microsoft, How do I check spelling in Outlook on the web? URL: https://support.office.com/en-gb/article/how-do-i-check-spelling-in-outlook-on-the-web-e1a30307-d751-4ce2-8eb3-b00d72cde1c5

[22] Microsoft, Editor is your writing assistant in Word, URL: https://support.office.com/en-gb/article/redacteur-is-uw-schrijf-hulp-in-word-91ecbe1b-d021-4e9e-a82e-abc4cd7163d7 On this support page, Microsoft incorrectly does not mention that the Editor function is also available in all Office for the Web applications (Word, Excel, PowerPoint, Outlook and Teams) and in Word on iOS.

[23] Microsoft, Insert data from picture, URL: https://support.office.com/en-gb/article/insert-data-from-picture-3c1bb58d-2c59-4bc0-b04a-a671a6868fd7

[24] Microsoft, Change handwritten ink to shapes, text or math in PowerPoint for Office 365, URL: https://support.office.com/en-gb/article/change-handwritten-ink-to-shapes-text-or-math-in-powerpoint-for-office-365-0740dec3-6291-4c1f-8baa-011d18449919

[25] Microsoft, Present with real-time, automatic captions or subtitles in PowerPoint in PowerPoint, Web, URL: https://support.office.com/en-gb/article/present-with-real-time-automatic-captions-or-subtitles-in-powerpoint-68d20e49-aec3-456a-939d-34a79e8ddd5f?ui=en-US&rs=en-US&ad=US

	Make professional slide-formats with PowerPoint Designer.[26]
Scan business card	Available in Outlook on Android. Use Office Lens to scan a business card and to add a contact person to Outlook Mobile. [27]
Calendar apps	Available in Outlook for Android and iOS.[28]
Convert to webpage	Available in Word for the Web. Convert a Word-document to a webpage for Sway.[29]
Translator	Available in Word, PowerPoint, Outlook and Excel for the Web, also in mobile Office apps. Translate text in a different language.
Frequently Asked Questions	Available in Outlook for iOS and Android, below Settings > Help and Feedback > Frequently Asked Questions
Inked effects	Available in Excel, Word and PowerPoint for iPad, Excel Word and PowerPoint for iPhone, Word, Excel and PowerPoint for Android-tablets, Excel Word and PowerPoint for Android-telephones. Drawing and writing with inked in Office.[30]
Insert Pictograms	Available in PowerPoint for the Web, Excel, Word and PowerPoint for iPad and for iPhone. Insert Pictograms in Microsoft Office.[31]
Office Help	Available in Office for the Web. When you choose Help > Help in the ribbon or use F1 in an Office-app.
Search for online-shapes (Visio)	Available in Office for the Web. Search more shapes and stencils.[32]
Explanation	Available in all inspected Office for the Web and mobile applications. Get started with Explanation, recognisable by the text field 'Show me what you want to do'.[33]
Use @mention to tag someone	Available in Excel, Word and PowerPoint for the Web, Excel, Word, PowerPoint for iPad and iPhone, Word,

[26] Microsoft, Create professional slide layouts with PowerPoint Designer, URL: https://support.office.com/en-gb/article/create-professional-slide-layouts-with-powerpoint-designer-53c77d7b-dc40-45c2-b684-81415eac0617?ui=en-US&rs=en-US&ad=US
[27] Microsoft, Scan or tap to add contacts, URL: https://support.office.com/en-gb/article/video-scan-or-tap-to-add-outlook-mobile-contacts-4818ef14-0fc8-4ec2-bb4d-440ea8cae17b?ui=en-US&rs=en-US&ad=US
[28] Microsoft, What are Calendar Apps? URL: https://www.osupportweb.com/a/outlook-mobile/?p=android&s=getting-started-on-outlook&f=what-are-calendar-apps
[29] Microsoft, Transform your Word document into a Sway web page, URL: https://support.office.com/en-gb/article/een-word-document-omzetten-in-een-sway-webpagina-65912b2d-8b81-41e1-ac52-c20a65ce8ecf?ui=nl-NL&rs=nl-NL&ad=NL
[30] Microsoft, Draw and write with ink in Office, URL: https://support.office.com/en-gb/article/draw-and-write-with-ink-in-office-6d76c674-7f4b-414d-b67f-b3ffef6ccf53?ui=en-US&rs=en-US&ad=US
[31] Microsoft, Insert icons in Microsoft Office, URL: https://support.office.com/en-gb/article/insert-icons-in-microsoft-office-e2459f17-3996-4795-996e-b9a13486fa79?ui=en-US&rs=en-US&ad=US
[32] Microsoft, Find more shapes and stencils, URL: https://support.office.com/en-gb/article/find-more-shapes-and-stencils-0475ddea-2a0a-4dec-ab8c-7dda9e63bca9?ui=en-US&rs=en-US&ad=US#ID0EBABAAA=Web
[33] Microsoft, Do things quickly with Tell Me, URL: https://support.office.com/en-gb/article/do-things-quickly-with-tell-me-f20d2198-17b8-4b09-a3e5-007a337f1e4e?ui=en-US&rs=en-US&ad=US

	Excel and PowerPoint for Android-tablets and for Android-telephones.[34]
Chat in Microsoft Office	Available in Excel, Word and PowerPoint for the Web.[35]
Inbox with priority	Available in Outlook for the Web.[36]
Apply sensitivity labels to your documents and email	Available in Excel, Word, PowerPoint and Outlook for the Web, Excel, Word and PowerPoint for iPad, iPhone, Android-tablets and Android-telephones.[37]
Share a document	Available in Excel, PowerPoint and Word for the Web.
View documents which others shared with you	Available in Excel, PowerPoint and Word for the Web, Excel, Word and PowerPoint for iPad and iPhone and Word, Excel and PowerPoint for Android tablets and telephones.[38]
Team mailboxes	Available in Outlook for the Web.[39]
Display prior versions of Office-documents	Available in Word for the Web.[40] View prior versions of documents which are saved in SharePoint for the Web or OneDrive for Business.
Receive a notification when members of your team edit your shared document	Available in PowerPoint, Excel and Word for the Web and PowerPoint for iPad and iPhone, Word, Excel and PowerPoint for Android-tablets and Excel, OneDrive, PowerPoint and Word for Android-telephones.[41]

The following Processor Connected Experiences are **not available** in the tested versions of Office for the Web and the mobile Office apps: PowerPoint Quickstart, 2D Mapping (creating geographical map charts in Excel), 3D maps, Automatic alternative text, Ideas in Excel, Maps in Power View in Excel, Online Presentation in PowerPoint, Publish to Power BI from Excel, Publish to Microsoft Stream from PowerPoint, Tap for Word (add from files), Data type shares and geography in Excel, Insert Microsoft Forms in PowerPoint, Choose Map in Outlook for iOS and Android, PowerPoint Quickstart, Researcher for Word and Free, Download ready-to-use templates for PowerPoint, Create a brainstorm diagram in Visio, Soon available in Outlook, Import

[34] Microsoft, Use @mention in comments to tag someone for feedback, URL: https://support.office.com/en-gb/article/use-mention-in-comments-to-tag-someone-for-feedback-644bf689-31a0-4977-a4fb-afe01820c1fd?ui=en-US&rs=en-US&ad=US
[35] Microsoft, Enhance collaboration with Chat in Microsoft Office, URL: https://support.office.com/en-gb/article/enhance-collaboration-with-chat-in-microsoft-office-1ecc6c7f-0b02-4baa-b9d9-c9d67023bedd?ui=en-US&rs=en-US&ad=US
[36] Microsoft, Focused Inbox for Outlook, URL: https://support.office.com/en-gb/article/focused-inbox-for-outlook-f445ad7f-02f4-4294-a82e-71d8964e3978?ui=en-US&rs=en-US&ad=US#bkmk_web
[37] Microsoft, Apply sensitivity labels to your files and email in Office, URL: https://support.office.com/en-gb/article/apply-sensitivity-labels-to-your-files-and-email-in-office-2f96e7cd-d5a4-403b-8bd7-4cc636bae0f9?ui=en-US&rs=en-US&ad=US
[38] Microsoft, See files others have shared with you, URL: https://support.office.com/en-gb/article/see-files-others-have-shared-with-you-e0476dc7-bf2f-4203-b9ad-c809578b03e7?ui=en-US&rs=en-US&ad=US
[39] Microsoft, Site mailboxes, URL: https://support.office.com/en-gb/article/sitemailboxes-a9c4b8c7-a1a9-43c0-bd05-7513ca092863?ui=en-US&rs=en-US&ad=US
[40] Microsoft, View previous versions of Office files, URL: https://support.office.com/en-gb/article/view-previous-versions-of-office-files-5c1e076f-a9c9-41b8-8ace-f77b9642e2c2?ui=en-US&rs=en-US&ad=US
[41] Microsoft, Get notified when members of your team update your shared file, URL: https://support.office.com/en-gb/article/get-notified-when-members-of-your-team-update-your-shared-file-9cc94893-02d5-4d96-9b3f-8b9414d5047a?ui=en-US&rs=en-US&ad=US

data in shapes in your drawing in Visio, Visualize data in Visio, Design flows in Visio, Organigram in Visio, Import and export timeline data between Visio and Project, Connect an external list to Outlook, Open a restricted permissions file (Information Rights Management), Open recent files from the File menu and Manage space search in Outlook.

New Connected Experiences

Microsoft regularly adds new Connected Experiences to its Office applications. These Connected Experiences are usually turned 'On' by default. Because Microsoft itself does not distinguish between Processor Connected Experiences and Controller Connected Experiences and the list of types of Connected Experiences is not complete, it is not clear in which role and for which purposes Microsoft processes personal data from and about the use of these services. In the test setup, all Connected Experiences were switched off for the mobile Office apps (see figures 8, 9 and 10 in section 3.1). In Office for the Web there is only one control for administrators: to turn off the Controller Connected Experiences. Without the central opt-out for the Connected Experiences, these services are all on, except for the use of the browser location.

Recently, Microsoft added three new Connected Experiences to Outlook for the Web, as set out in the figure below. As these Connected Experiences are not included in the list of Additional Optional Connected Experiences, these services must be Processor Connected Experiences.

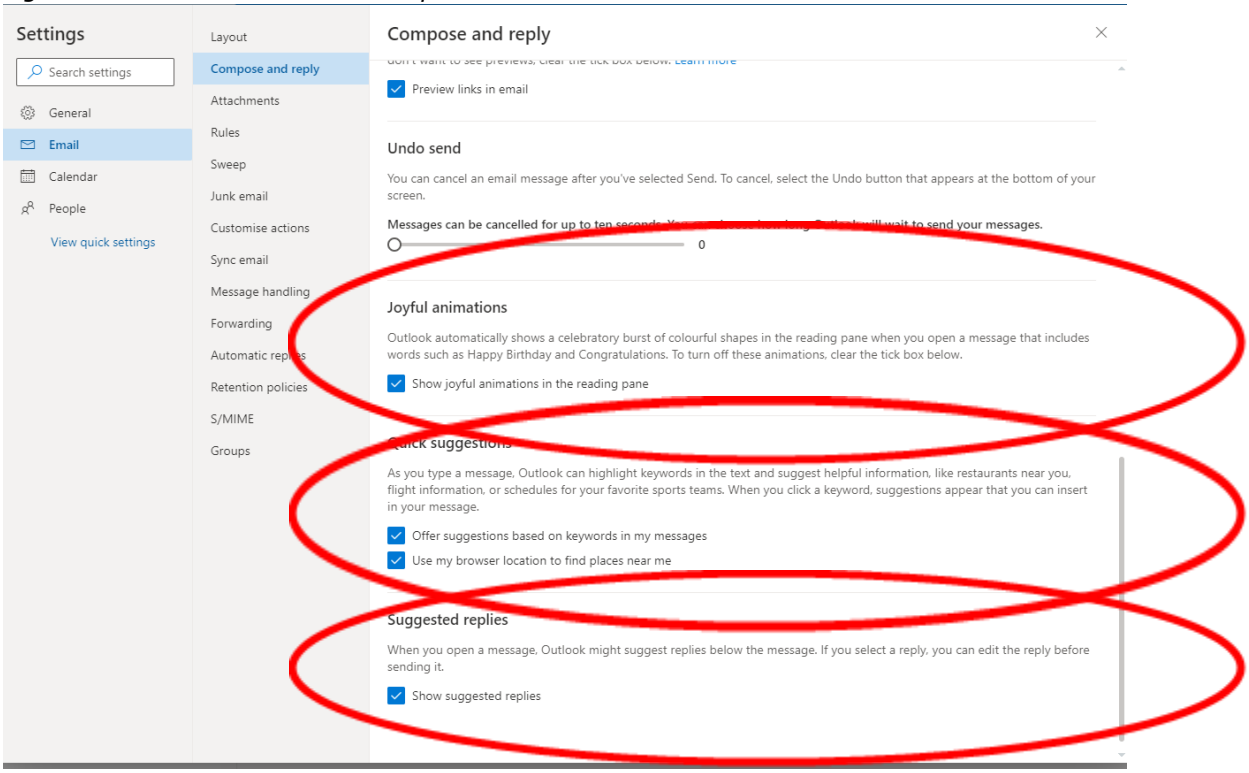
The 'Joyful animations' option means that a virtual glitter shower appears in Outlook for the Web if the software recognises words such as 'birthday' or 'congratulations'.[42] The 'Quick suggestions' option also recognises keywords from messages in order to make (commercial) suggestions for restaurants in the neighbourhood.

Microsoft explains that it uses computer algorithms to recognise the content of messages and machine learning technologies to provide response options: "*Suggested responses are generated by a computer algorithm and use natural language processing and machine learning technologies to provide response options.*"[43]

[42] Source: Howtogeek, URL: https://www.howtogeek.com/424734/how-to-turn-off-outlook.coms-new-joyful-animations/ *"Microsoft recently added "joyful animations" to the Outlook web app. These show a shower of glitter whenever Outlook detects "joyful" words like "Congratulations" or "Happy Birthday."*

[43] Microsoft, Use intelligent technology in Outlook on the web, URL: https://support.office.com/en-gb/article/use-intelligent-technology-in-outlook-on-the-web-24b30683-8340-4b69-b8ac-4193ec528a70

Figure 2: Three new Connected Experiences to Outlook for the Web



Cloud Connected Services

Azure AD

Generally, identity details of Dutch government employees 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 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 because the service offers extensive possibilities for adding, updating and deleting users, registering devices and managing the authorisations per user.[44] Through the Azure AD, Microsoft processes the account data of employees and students in either case. If educational institutions make use of cloud services in the future, Microsoft can use the Azure AD to collect more data about work patterns (log-in and log-out times). This is explained in section 8 of this report.

Exchange Online

Exchange Online is Microsoft's cloud-based mail server.

SharePoint Online / OneDrive for Business

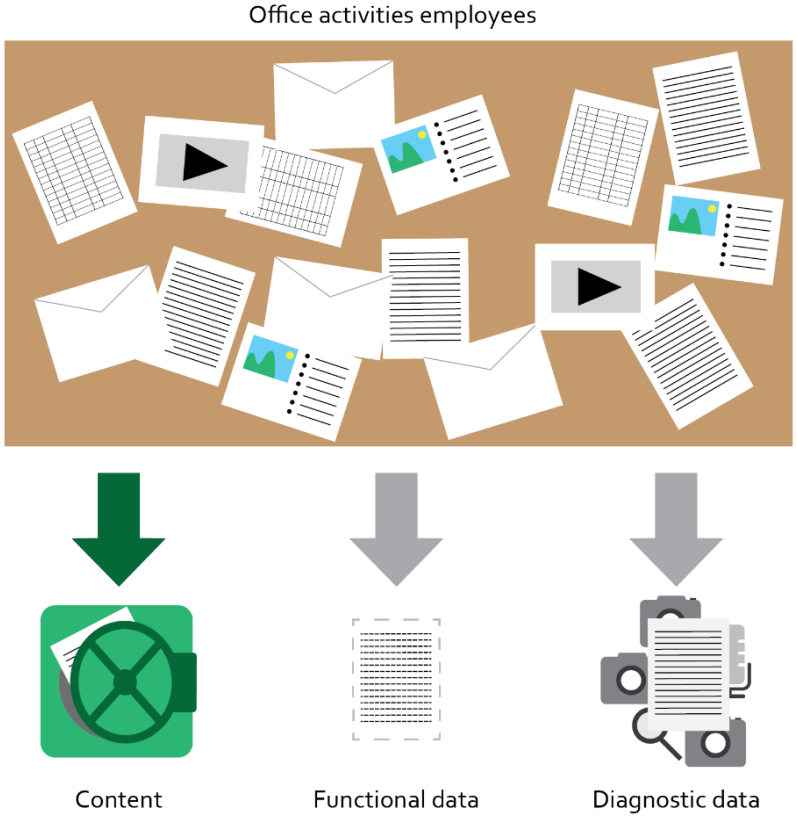
SharePoint Online and OneDrive for Business from Office for the Web offer cloud storage space. This allows employees to store and share files with each other more easily from the Office software.

[44] See the explanation of Microsoft, Microsoft Cloud Identity for Enterprise Architects, August 2016, https://www.microsoft.com/en-gb/download/confirmation.aspx?id=54431&6B49FDFB-8E5B-4B07-BC31-15695C5A2143=1

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:

Figure 3: Content data, functional data and diagnostic data



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 subject lines of emails sent via Exchange Online.

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.

Functional data, which are only necessary for the transfer of communication. This data should be deleted or anonymised directly after completion of the transfer of communication, according to the e-Privacy directive.

In this report, all data about the individual use of the mobile Office apps, Office for the Web, the use of the Connected Cloud Services and the Connected Experiences 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.
The term functional data is used for all data that must be sent from the user's device to communicate with services on the Internet, including Microsoft's own apps and services. Examples of such functional data are the data processed by an email server, and the data stream necessary to allow the user to authenticate or to verify if the

user has a valid license. Functional data may also include snapshots that Microsoft collects about the configuration of the Office software to provide updates. This category of data can also include the contents of a query in search engine Bing, or the content of text a user wants to have translated. In that case, Microsoft may collect the sentence before, and after the sentence marked by a user for translation, to provide a better translation. Functional data may thus include content data.

The main difference between functional data and diagnostic data as defined in this report, is that functional data are and should remain transient.[45] 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 Office for the Web applications and the mobile Office apps, the Connected Experiences and the Connected Cloud Services. 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 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 lines of text from the content of documents of which spelling is checked online, file and path names when using SharePoint Online and OneDrive for Business, and mail headers when using the online mail server Exchange Online. There is a fourth category of metadata; about the use of the online authentication service Azure Active Directory. These two types of processing are further explained in section 8 of this report.

Microsoft systematically collects data about the use of its software. With the installed versions of the software (ProPlus and the mobile Office apps, but recently also via the browser in Office for the Web), Microsoft does this 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. These 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 it possible for end-users to view the data themselves in 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. Since February 2020, Microsoft has made the Data Viewer suitable for telemetry from three mobile Office apps: Word, PowerPoint and Excel. This Data Viewer Tool is not available for

[45] 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.*"

the telemetry events from Office for the Web. In its response to the technical findings from this DPIA, Microsoft indicated that there is no possibility to view the telemetry data from Office for the Web, because these are so-called *required data*.

On mobile devices, Microsoft has less control over the operating system (limited to iOS and Android in this report). Messages about individual usage are sent to Microsoft, but less events than from the desktops and laptops. Users see this traffic from three mobile Office apps via the Data Viewer Tool, if they also have a device with Windows 10 as the operating system. Privacy Company carried out test scenarios on two test phones, intercepted the outgoing traffic and decrypted the contents of the telemetry events in the best possible way.

In the Office for the Web applications, which run in a user's browser, Microsoft also collects telemetry events (since September 2019). In addition, Microsoft collects personal information about the use of these applications in log files of its cloud servers. Microsoft records those usage data in so-called system-generated event logs. These logs do not just contain data about the use of Office for the Web, but also data about the use of the Connected Experiences and other Microsoft Online Services such as the Azure Active Directory, SharePoint Online and OneDrive, and the cloud mail server Exchange Online.

In order to gain access to the data that Microsoft collects about the individual use of its Online Services, Privacy Company inspected the audit logs available for system admins and used Microsoft's Data Subject Access Request tool to request access to the diagnostic data of the two test accounts.

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.

The section about personal data provides legal, technical and organisational arguments why the diagnostic data processed by Microsoft about the individual use of Office for the Web, the mobile Office apps, the Connected Experiences and the use of the Connected Cloud Services.

In sections 2.3 and 2.6 the captured traffic to third parties is described from respectively the mobile Office apps and Office for the Web.

This section also provides a technical analysis of the telemetry data from the mobile Office apps, the results of the different data subject access requests for the diagnostic data and the outcomes of a Content Search for the diagnostic data relating to the use of the cloud storage and email services.

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 Microsoft Rijk concluded with Microsoft, 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).[46]

In its new DPA of January 2020, under the heading 'Processing of Personal Data; GDPR' Microsoft explains: *"All Personal Data processed by Microsoft in connection with the Online Services is obtained as* ***Customer Data, Diagnostic Data, or Data Generated by the Service. Personal Information provided to Microsoft by or on behalf of a Customer through use of the Online Service is also Customer Information.*** *There may also be pseudonymized identifiers contained in Diagnostic Data or Service Generated Data, and these are also Personal Data. Pseudonymised Personal Data, or Personal Data that has been stripped of its identity features but has not been anonymised, or Personal Data derived from Personal Data, are also Personal Data."*[47]

In this DPA Microsoft also provides new definitions of diagnostic data on the one hand (telemetry) and service generated logs on the other hand.

""Diagnostic Data" means data collected or obtained by Microsoft from software that is locally installed by Customer in connection with the Online Service. Diagnostic Data may also be referred to as telemetry. Diagnostic Data does not include Customer Data, Service Generated Data, or Professional Services Data."

"Service Generated Data" means data generated or derived by Microsoft through the operation of an Online Service. Service Generated Data does not include Customer Data, Diagnostic Data, or Professional Services Data.

[46] Microsoft Online Services Data Protection Addendum, January 2020, URL: https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=15981 Though Microsoft updates its OST on a monthly basis, this does not seem the case for the DPA.
[47] Ibid.

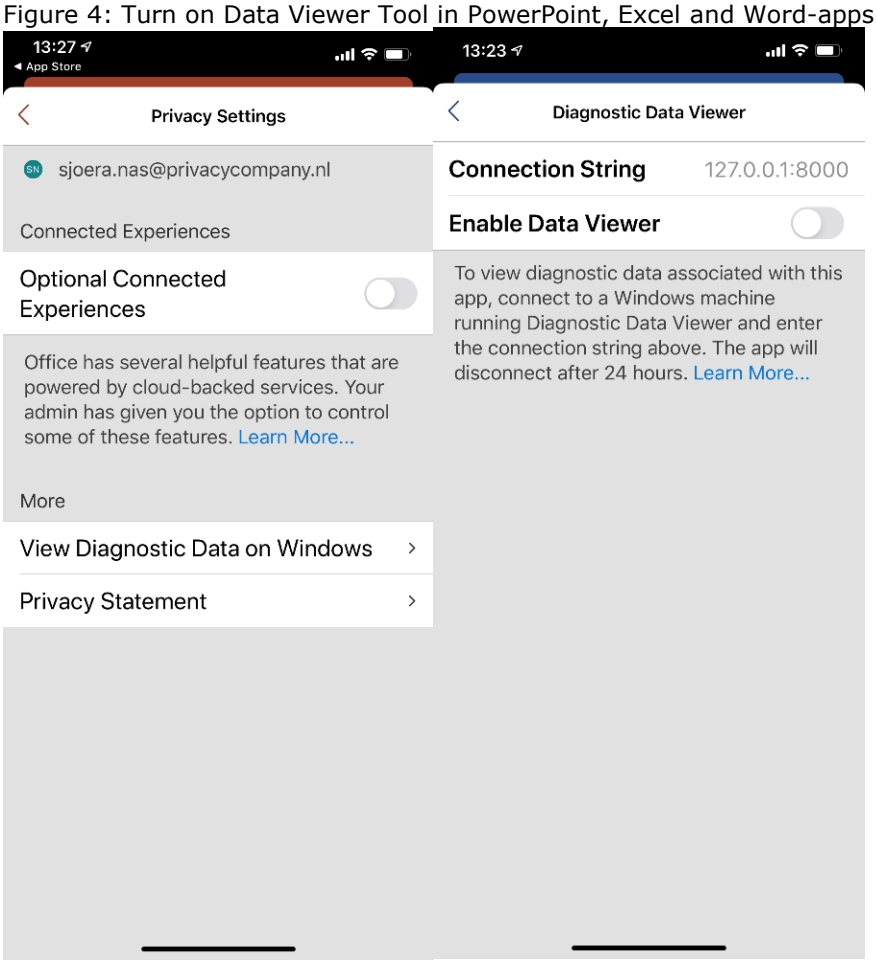
For Enterprise customers that cannot benefit from the Dutch government's privacy amendment, it is a major improvement that Microsoft describes that the processing of diagnostic data or the processing of data generated by the service can both be processing of personal data, even if pseudonymised data are generated through the use of online services. It is also an improvement that Microsoft gives a number of examples of data that are still personal data, despite scrubbing, or because they are *derived* from other personal data.

2.2 Diagnostic data mobile Office apps

Microsoft has included a telemetry client in the Office apps and -since recently- in Office for the Web. Microsoft has programmed that client to collect telemetry data on the device and send it *in batches* to Microsoft on a regular basis.

The data collection via the mobile Office apps is not transparent. Microsoft does not publish any information about the telemetry data it collects about the use of the mobile Office apps (nor about Office for the Web). Microsoft has offered a Data Viewer Tool for telemetry traffic from Office 365 ProPlus since June 2019. As quoted in the Introduction, Microsoft writes in its response to the technical finding in this report that the Data Viewer Tool should work *in the main iOS* [and Android] *applications used by organisations and in Office for the Web*. However, this research shows that the tool is not available, or does not function yet, in the Outlook, Teams, OneDrive and OneNote mobile Office apps.

Figure 4: Turn on Data Viewer Tool in PowerPoint, Excel and Word-apps on iOS.



Aside from the absence of a Data Viewer Tool for the mobile Outlook, Teams, OneDrive and OneNote apps, Microsoft does not actively inform data subjects and admins that it collects data via the mobile Office apps about the individual use of these apps. The information is not present in the apps, not in the app stores and not in the general information pages published by Microsoft. Microsoft also does not offer a choice to end-users to minimise this data flow, as has been the case for Office 365 ProPlus since the end of May 2019 and for Windows 10 since May 2018.

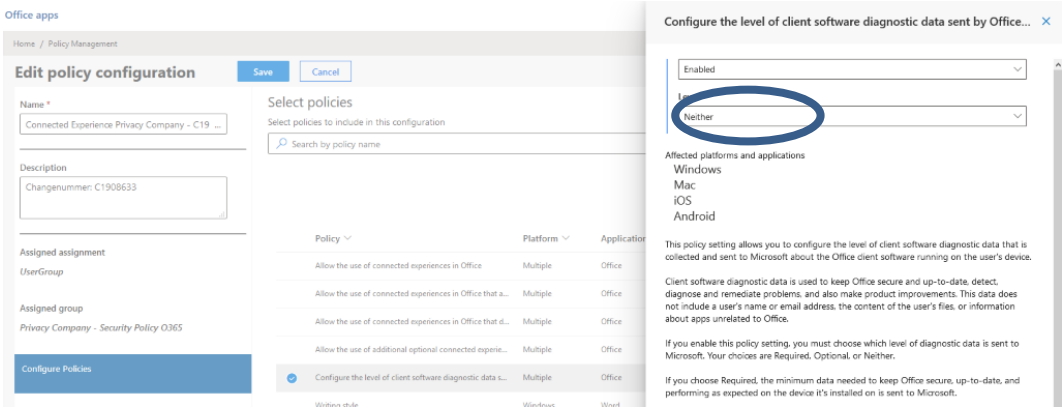
As described in Appendix 1, it was technically not possible to fully analyse the captured data from the mobile devices. Because Microsoft has not published documentation with the specifications of the binary format in which it enciphers the data, Privacy Company has made a best effort to distil the contents from the collected telemetry data. This was more difficult on Android devices, than on iOS devices.

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 shows that all events from the mobile Office apps on the two operating systems at least contain the device identifier DeviceInfo.Id. The telemetry also contains a field 'UserInfo.Id' that contains two types of identifiers, depending on whether Microsoft qualifies the account as a Business account or as a Consumer account. The distinction is remarkable, because the researchers were always logged in with a Work 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.

Since the autumn of 2019 or January 2020 (depending on the update regime used by the administrators for Office 365 updates), Microsoft does offer system administrators of the Enterprise and Edu versions of the Office 365 software the option of minimising the level of telemetry in the mobile Excel, PowerPoint and Word apps. See Figure 5 below. For this DPIA the telemetry level was set to the lowest level: 'Neither'.

Figure 5: telemetry level configuration



Microsoft announced in September 2019, on its information page about the Office 365 ProPlus telemetry data, that it intended to extend the enhanced privacy controls to additional Office [software] clients, including Teams and the mobile Office apps, in the *coming months*. The improvements should not only introduce an ability to set the telemetry level, but also to disable some or all Connected Experiences.[48] At the time of completion of this DPIA, end of March 2020, a privacy control for end-users to disable the Connected Experiences is only available in the Word, PowerPoint and Excel mobile Office apps (if access to the Connected Experiences has not been forbidden by their administrator).

Microsoft writes:
"These privacy controls are included in Version 1908 of Semi-Annual Channel (Targeted), which was released on September 10, 2019. They are expected to be available in Semi-Annual Channel in January 2020.
These privacy controls are available for Version 2.30 and later of ***the iOS versions of Excel, OneNote, PowerPoint, and Word****, as well as Version 1.17 and later of Visio Viewer for iOS.*
These privacy controls are available for Version 16.0.12226.10000 and later of ***the Android versions of Excel, PowerPoint, and Word****, as well as Version 16.0.12228.20004 and later of OneNote for Android.*
Most of the Office for the web applications are scheduled to start using the new privacy control for optional connected experiences in mid-October 2019. Those applications are the following: ***Excel for the web, OneNote for the web, PowerPoint for the web, Visio for the web, and Word for the web.*** *Before that starts, you can use the Office cloud policy service to configure the appropriate policy setting.*
We will be extending these new and improved privacy controls to additional Office clients, including Teams and our mobile Office apps. We'll provide more information about those changes in the upcoming months. We will continue to carefully listen to your feedback and make improvements across all Office 365 clients and services."[49]

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 telemetry events.

The investigation of the **iOS and Android mobile Office apps shows that Microsoft does not collect any content data from the content of files, email or chats via the telemetry events, nor any file or path names, when the telemetry is set to the lowest 'Neither'.** Microsoft therefore processes far fewer types of diagnostic events via the mobile Office apps than via the installed ProPlus version of Office 365. In the ProPlus version, Microsoft initially collected 23,000 to 25,000 different types of events. Microsoft's public documentation on the privacy improvements implemented in the spring version of Office 365 ProPlus shows that this number has also been substantially reduced. Microsoft describes just over a hundred different types of telemetry events about content actions, each of which can consist of up to 100 fields, and 8 events from the header. **Please note** that some telemetry events from **Office for the Web (Word and PowerPoint) do contain content data such as username, path and file name.** This is discussed in section 2.4.

[48] Microsoft Deploy Office, Privacy voor Office 365 ProPlus / Overview of the privacy-settings, Overview of privacy controls for Office 365 ProPlus, 8 November 2019, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/overview-privacy-controls
[49] Ibid.

2.3 Outgoing traffic to third parties mobile Office apps

Microsoft sends personal data via the mobile Office apps to the German company Adjust (via the OneDrive and Outlook apps) to four American companies and to its own subsidiary Hockeyapp. Traffic is sent from the mobile Word app to Cloudflare, from the Outlook app to Helpshift and UserVoice and from the Teams app to Giphy.

This traffic and the ratio of the use of these companies by Microsoft is explained per party below, with the exception of Hockeyapp.

There is a difference between the mobile Office apps and Office for the Web. Microsoft does not publish any information about the parties with whom it collaborates in providing its consumer services. Microsoft counts the mobile Office apps among its consumer services. This will be explained in more detail in section 5.3 of this report (*Data Controller*).

Microsoft publishes an exhaustive list of subprocessors for its Online Services. It includes 13 technology providers and six companies providing 'support' services such as helpdesk services. Microsoft also mentions a number of subprocessors that provide support staff on this list.[50] New subprocessors have to be approved in accordance with the procedure in the Online Service Terms and the Data Protection Addendum, as amended by the agreement with SLM Microsoft Rijk of May 2019. A new subprocessor may only be added after a notice period, during which a customer can object to the appointment of the subprocessor.

In its general privacy statement (which applies to the mobile Office apps), Microsoft explains that it may share personal data with third parties such as affiliates and vendors, but that these companies must comply with Microsoft's security and privacy requirements.

Microsoft writes in this consumer oriented privacy statement: "*In addition, we share personal data among Microsoft-controlled affiliates and subsidiaries. We also share personal data with vendors or agents working on our behalf for the purposes described in this statement. For example, companies we've hired to provide customer service support or assist in protecting and securing our systems and services may need access to personal data to provide those functions. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose. We may also disclose personal data as part of a corporate transaction such as a merger or sale of assets.*"[51]

The fact that Microsoft requires such third parties to comply with Microsoft's rules does not mean that Microsoft has a processor agreement with those parties as referred to in Article 28 of the GDPR.

Microsoft has responded on 6 March 2020 to the observation of this outgoing traffic from the mobile Office apps.

[50] Microsoft Online Services Subprocessors List, last available version September 2019, accessible via Microsoft Data Protection Resources: https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3 (tab most right)
[51] Microsoft general privacy statement, last updated in February 2020, URL: https://privacy.microsoft.com/en-gb/privacystatement

"The observation of data traffic does not mean subprocessing of customer content or personal data is occurring or that Online Service outcomes are being provided by Microsoft. Microsoft uses internal software logic to enforce that when data processing is performed with Office 365 work or school accounts that any subprocessing of personal data and customer content is limited to the disclosed subprocessors.

Many of the listed examples are providing functionality unrelated to Online Services.

1. *Support engagement via Helpshift is optional for the customer and the user and provides support for the app and not the Online Services.*
2. *Providing feedback by UserVoice is optional for the user and organisation and is not an Online Service data processing outcome by Microsoft.*
3. *As discussed above, Giphy is an optional third party experience available to users under Giphy's terms and privacy policy. As part of its effort to give service administrators greater configurability, system administrators have the option to disable use of Giphy in Teams, where Giphy is present as an option."*[52]

In an earlier response of Microsoft to SLM Microsoft Rijk, as published in the earlier public DPIA about Office for the Web and the mobile Office apps of July 2019, Microsoft wrote:

"*All Office Mobile applications are (indeed) offered under a EULA between Microsoft and the mobile device user, and the diagnostic data it collects is governed under the Microsoft Privacy Policy and the EULA. However, and crucially, data provided to Microsoft or collected by Microsoft through the use of an Azure AD Account authenticated in the Mobile apps are governed under the OST and your agreement.*"[53]

According to this statement, Microsoft should process all personal data that it collects via the mobile Office apps after logging in with an Azure AD account as a data processor, in accordance with the privacy terms and conditions negotiated by SLM Microsoft Rijk in May 2019. However, Microsoft's explanation that the traffic to third parties would not involve personal data contradicts the findings of this DPIA and is at odds with the information published by the third parties themselves. Unless the administrator has blocked the traffic (which is not available in respect of each third party), the relevant third party always receives personal data in the form of the IP address of the users, in combination with other data about the behaviour and/or device of the user.

2.3.1 Adjust

Privacy Company has detected traffic to the German company Adjust GmbH from the OneDrive and the Outlook app on iOS. This concerns the transfer of personal data, because the traffic contains at least the IP addresses of visitors. Appendix 1 explains why it was not possible to decode the traffic from the Android apps. However, Privacy Company has no reason to assume such traffic was not sent from the same Android mobile Office apps.

Adjust specialises in measuring the reach of, and combatting fraud with, mobile ads. The company indicates that it processes diagnostic data for four purposes: Event

[52] Email Microsoft to the researchers of 6 March 2020.
[53] Email Microsoft to SLM Microsoft Rijk van 19 July 2019, cited in the DPIA Microsoft Office 365 Online and Mobile, SLM Microsoft Rijk 23 July 2019, p. 31, 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

Tracking, Impression Tracking, Install Tracking and Retargeting. In its privacy policy, it states that it acts as a processor for app customers for the following purposes:
"*We use the aforementioned data for providing mobile analytics and attribution services to our Customers, and thereby allow our customers to track their marketing performance, to match You to their campaigns and to understand how You engage with our Customer's app. Furthermore, we enable our Customers to track Your interactions in their apps in real time in order to see how You engage over their full lifetime.*"[54]

For these purposes, Adjust processes the following types of personal data:
"*Our SDK and APIs (collectively the "adjust technology") may process some of the following data from You as the End User:*

1. *hashed IP address*
2. *Mobile identifiers such as the ID for Advertising for iOS (IDFA), Google Advertising ID or similar mobile identifiers*
3. *Installation and first opening of an app on Your mobile device*
4. *Your interactions within an app (e.g. in-app purchases, registration)*
5. *Information regarding which advertisements You have seen or clicked on*
6. *For the Unbotify/Fraud product additionally: sensory data including touch events, counting text changes, accelerometer, gyroscope, battery, light sensor, device hardware specifications and operating system version*."[55]

Adjust is not on Microsoft's list of subprocessors for the Online Services, as last updated on 5 September 2019.[56] Microsoft did not provide an explanation about this traffic in its response of 6 March 2020. The DPIA investigation shows that system administrators should be able to block the traffic to Adjust centrally by blocking the network endpoint (see paragraph 3.1 of this report). Microsoft mentions the domain app.adjust.com in its list of global network endpoints, as no. 110, with the following explanation: "*Default Optional, Notes: Outlook for Android and iOS: Adjust integration*".[57] The interpretation 'Optional' (instead of Required) means that the administrator should be able to block this traffic. Microsoft explains: "*For endpoint sets which are not required to have network connectivity, we provide notes in this field to indicate what functionality would be missing if the endpoint set is blocked.*"[58]

2.3.2 Akamai

Privacy Company has seen traffic from the Outlook and Teams apps on iOS to the domains spoprod-a.akamaihd.net, img-prod-cms-rt-microsoft-com.akamaized.net and statics-marketing sites-neu-ms-com.akamaized.net. This includes the transfer of personal data, because the traffic contains at least the IP addresses of visitors, geographical location, telemetry data and websites visited, plus any personal data contained in the contents of cached information.[59]

---

[54] Adjust privacy policy, 4. Processing of data through the Adjust Technology, last revised 27 November 2019, URL: https://www.adjust.com/terms/privacy-policy/
[55] Idem.
[56] Microsoft Trust Center, https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3 Version 5 September 2019, with a tab completely right with an overview of processors, with a hyperlink to:https://go.microsoft.com/fwlink/p/?linkid=2096306
[57] Microsoft, Office 365 Worldwide endpoints, URL: https://docs.microsoft.com/en-gb/office365/enterprise/urls-and-ip-address-ranges
[58] Idem.
[59] Akamai describes these data in the Data Processing Addendum as follows: *In providing services to Customer, Akamai may process one or more of the following categories of data:*

Akamai is a content delivery network. Akamai offers copies of information through a variety of self-owned data centres, as close to the users as possible to increase speed. Through these domains static content is retrieved (fonts, images, java scripts, etc.).

Microsoft has concluded a processor agreement with Akamai as a content delivery network for the online services according to the exhaustive list of subprocessors included in the Online Service Terms. However, it is not clear whether this subprocessor agreement also applies to traffic from the mobile Office apps, for which Microsoft acts as the (independent) controller contrary to the contractual agreement with SLM Microsoft Rijk.

2.3.3 Cloudflare

Traffic was captured to the U.S. company Cloudflare from the Word app on iOS. The traffic concerns the transfer of personal data, because it contains at least the IP addresses of visitors, plus log data.

Just like Akamai, Cloudflare is a content delivery network, providing its own DNS services. Cloudflare has its own data centres, for example in Amsterdam, and can therefore, just like Akamai, display locally stored copies of websites. Because the websites are already downloaded and compressed, the pages load faster. Cloudflare also provides security services, such as checking blacklists of the IP addresses of known hackers and spammers.[60] According to an article on its own website, Cloudflare provides DDoS protection for websites hosted in Microsoft Azure.[61]

According to its privacy statement[62] Cloudflare collects the following data about end users of its services, i.e. when people use the domains, websites or mobile Office apps of Cloudflare Customers (in this case: Microsoft):

(i) Personal Data in Customer Content: Personal data included within Customer Content that is cached or stored on Akamai's servers for purposes of optimization, is provided by a customer for storage on Akamai servers, or that otherwise transits the Akamai servers as part of a data subject's session with the customer's web property ("End User Personal Data"). End User Personal Data may include,
a. Login credentials
b. Subscriber name and contact information
c. Financial or other transaction information
d. Other information relating to the individual data subject as requested or provided by the customer through the use of its web property.
"Customer Content", means content and applications, including any third-party content or applications, provided to Akamai for delivery via or use by the Akamai network.
(ii) Personal Data in Akamai Logged Data: Akamai Network Data, logged by Akamai servers, relating to the delivery of information over the Akamai platform, as well as logged personal data associated with user activity and interaction with web and internet protocol sessions transiting Akamai's servers as part of a data subject's session with the Customer's web property ("Logged Personal Data"). Logged Personal Data may include,
a. End user IP addresses
b. Page activity data and URLs of sites visited with time stamps (when combined with an associated IP address)
c. Geographic location based upon IP address and location of Akamai server (no more granular than city level)
d. Telemetry data (e.g., mouse clicks, movement rates, and user agent and related browser data)."

[60] Dutch Blog Thomas van Eldijk, Cloudflare, wat is het? En wat zijn de voor- en nadelen? 1 februari 2019, URL: https://www.vaneldijk.nl/artikelen/cloudflare-wat-is-het-en-wat-zijn-de-voor-en-nadelen

[61] Cloudflare, URL: https://www.cloudflare.com/integrations/microsoft-azure/

[62] Cloudflare Privacy Policy, effective 31 October 2019, URL: https://www.cloudflare.com/privacypolicy/

"*This information may include but is not limited to IP addresses, system configuration information, and other information about traffic to and from Customers' websites or networks (collectively, "Log Data"). We collect and use Log Data to operate, maintain, and improve our Services in performance of our obligations under our Customer agreements.*"[63]

According to its privacy statement, Cloudflare can process personal data for the following purposes:

- *"Provide, operate, maintain, improve, and promote the Website and Services for all users of the Website and Services;*
- *Enable you to access and use the Website and Services;*
- *Process and complete transactions, and send you related information, including purchase confirmations and invoices;*
- *Send transactional messages, including responses to your comments, questions, and requests; provide customer service and support; and send you technical notices, updates, security alerts, and support and administrative messages;*
- *Send commercial communications, in accordance with your communication preferences, such as providing you with information about products and services, features, surveys, newsletters, offers, promotions, contests, and events about us and our partners; and send other news or information about us and our partners. See Section 9 below for information on managing your communication preferences.*
- *Process and deliver contest or sweepstakes entries and rewards;*
- *Monitor and analyse trends, usage, and activities in connection with the Websites and Services and for marketing or advertising purposes;*
- *Comply with legal obligations as well as to investigate and prevent fraudulent transactions, unauthorised access to the Services, and other illegal activities;*
- *Personalize the Websites and Services, including by providing features or content that match your interests and preferences; and*
- *Process for other purposes for which we obtain your consent."*[64]

Cloudflare writes that it acts as a processor for end users in the EU and only processes personal data on behalf of its customers. It is not clear whether or not the above purposes are permitted by Microsoft.

Cloudflare uses both the Privacy Shield and Standard Contractual Clauses for the transfer of personal data to the US.[65]

Cloudflare is not on Microsoft's list of subprocessors for the Online Services.[66]

Cloudflare does not appear on Microsoft's list of worldwide endpoints for Office 365 traffic. Microsoft did not provide an explanation for this traffic in its response of 6 March 2020. The investigation has shown that there is no possibility for administrators to centrally block the traffic to Cloudflare.

2.3.4 Giphy

[63] Idem.
[64] Idem.
[65] Idem.
[66] Microsoft Trust Center, URL: https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3 Version 5 September 2019, tab right.

When using Teams on iOS and Android, Microsoft sends personal data to the U.S. company Giphy, based in New York with a representative in Hamburg. Giphy offers a large collection of images (GIFs and animated GIFs) that users can insert into all kinds of chat programs and social media.

Traffic is sent to Giphy the moment a user inserts an image into a Teams Conversation. The request is automatically sent to Giphy, without the user getting any information or having a choice.

Giphy explains in its Privacy Statement[67] that it automatically collects the IP address, unique device identifier, cookie information and the specific advertising identifiers of Android and iOS from each user of its services. "*We automatically receive and record information from your web browser or device when you interact with the Services, including your IP address, device ID, and cookie information (..) We may also collect advertising identifiers from your mobile device.*"[68]

Giphy reserves the right to use the IP address for targeted advertising: "*Your IP address may be used to send you geographically-targeted advertisements.*"[69]

Moreover, Giphy allows itself to send secret pixels of advertising networks via the images. "*To increase the effectiveness of ad delivery, we may deliver a file (known as a "web beacon") from an ad network to you through the Services. Web beacons allow ad networks to provide anonymized, aggregated auditing, research and reporting for us and for advertisers. Web beacons also enable ad networks to serve targeted advertisements to you when you visit other websites.*"[70] For users in the EU, Giphy writes that she is not a processor, but controller: "*We will be the controller of your Personal Data processed in connection with the Services.*"[71]

Giphy relies on the EU-U.S. Privacy Shield Framework for the transfer of personal data from the EU to the US.[72]

The use of Giphy is not an Additional Optional Controller Experience. Giphy is also not on Microsoft's list of subprocessors for the Online Services.[73]

Microsoft does not list Giphy's domains in its list of global network endpoints.[74] However, tests executed for this DPIA show that it is possible for system administrators to centrally block the traffic to Giphy with a group policy.

2.3.5 Helpshift

Traffic, including personal data, was captured to the U.S. company Helpshift from the Outlook app on iOS, to the domain acompli.helpshift.com.

[67] Giphy privacy policy, effective date: August 28, 2019, Last Updated December 13, 2019, URL: https://support.giphy.com/hc/en-gb/articles/360032872931
[68] Idem.
[69] Ibid.
[70] Ibid.
[71] Ibid.
[72] Ibid.
[73] Microsoft Trust Center, https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3 Version 5 September 2019, with a tab completely right with an overview of processors, with a hyperlink to: https://go.microsoft.com/fwlink/p/?linkid=2096306
[74] Microsoft, Office 365 Worldwide endpoints, URL: https://docs.microsoft.com/en-gb/office365/enterprise/urls-and-ip-address-ranges

Helpshift, based in San Francisco, provides tools to improve customer service. Helpshift publishes a special case study on its website about its collaboration with Microsoft.[75] In it, Helpshift describes that it processes personal data from Outlook (user and device data):

"*With more than 75 million monthly users, Microsoft Outlook's in-app customer support efficiently addresses user issues at scale. Outlook benefits immensely from Helpshift's effective self-service options and automatically-collected user and device data. With the support platform's modern messaging and sophisticated routing, the Outlook team is able to respond to most issues within two hours, maintain a 4+ CSAT rating, and keep the cost of each chat under $1.*"

In the privacy policy, Helpshift writes that it can conversate via an in-app helpdesk for controllers: *In the course of using our Services, our customers and their end-users may submit or upload certain content, communications, data, attachments or files to our Services for hosting and processing by us. For example, if an end-user communicates with our customer's support staff using Helpshift's In-App Chat features, then we will process the end-user's name, email address and support request on behalf of our customers (as a data processor) and in accordance with their instructions. Our privacy practices in such cases will be governed by the contract that we have in place with them."*[76]

Helpshift describes that it can use cookies and beacons for various purposes, such as personalising the content of web pages but also to display targeted ads.[77]

On the information page about the Additional Optional Connected Experiences, Microsoft mentions the collaboration with a Microsoft owned service called Powerlift for Outlook, explicitly referring users to Microsoft's consumer terms and conditions and privacy policy. "*On Outlook for iOS and Android, you can report issues and connect with our support team through* ***Settings*** *>* ***Help & Feedback*** *>* ***Contact Support****. This experience requires a Microsoft owned service called PowerLift, and the terms of the Microsoft Services Agreement and Microsoft privacy statement apply.*"[78] Microsoft does not mention Helpshift.

Helpshift is not on Microsoft's list of subprocessors for the Online Services.[79] Helpshift is listed on the worldwide list of network endpoints as 'Default Optional'. Therefore, it should be possible for administrators to centrally block the traffic to Helpshift.

2.3.6 UserVoice

Traffic, including personal data, was sent to UserVoice in Outlook on iOS to the domain by.uservoice.com.

---

[75] Helpshift, How Microsoft's Outlook on User Feedback Creates Happier Customers at a Dramatically Reduced Cost, URL: https://www.helpshift.com/resources/case-study-how-microsofts-outlook-on-user-feedback-creates-happier-customers-at-a-dramatically-reduced-cost/

[76] Helpshift privacy effective date 27 March 2018, URL: https://www.helpshift.com/legal/privacy/ *For the purposes of European Data Protection Law, the Data Controller of EEA individual's personal information Helpshift, Inc.* https://www.helpshift.com/company/contact-us/ explains where Helpshift Inc is located: Helpshift Headquarters 343 Sansome Street, 5th Floor, San Francisco, CA 94104.

[77] Idem.

[78] https://docs.microsoft.com/nl-nl/deployoffice/privacy/optional-connected-experiences

[79] Microsoft Trust Center, https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3 Version 5 September 2019, with a tab completely right with an overview of processors, with a hyperlink to https://go.microsoft.com/fwlink/p/?linkid=2096306

UserVoice is an American company (based in Raleigh and San Francisco[80]) that specialises in digital customer research. The company describes itself as follows: "*a product management platform that enables product teams to make data-driven decisions about what they build based on customer feedback.*"[81]

The company has published a case study on working with Microsoft to better assess the priority of customer improvement requests in the Service Center Configuration Manager and Microsoft Intune.[82]

UserVoice describes its operations as follows: "*UserVoice helps them hear directly from all of their customers, and gives them both the data and context they need to build products their customers love. Both Intune and Configuration Manager have large communities of followers who actively share their ideas on how to make the product better. UserVoice aggregates feedback from all these customers into a single place, streamlining workflows for the Program Managers who are tasked with carefully listening to what customers are saying and reporting key findings to the leadership team."*[83] Based on this description the conclusion can be drawn that UserVoice combines diagnostic data with questions/complaints that users publish on the Internet.

The case study shows that other Microsoft teams, apparently including the product developers of the Outlook app for iOS, were already using UserVoice: "*The teams at Intune and Configuration Manager implemented UserVoice after hearing success stories from several other teams at Microsoft using the platform.*"

From the case study it appears as well that Microsoft can identify individual clients, about whom UserVoice processes data: "***I was then able to use UserVoice to identify customers, I was able to send all 53 supporters of this item an email and get more context***. *It wasn't on our radar at all before but now it's on our things to do." says Tyler Castaldo, Program Manager."*[84]

In its privacy statement, UserVoice describes the purposes of the data processing as follows[85]: "*UserVoice uses the information it collects from you to deliver UserVoice Services to you and continuously enhance your user experience. Generally speaking, we use the collected information to communicate with you, fulfil your requests, customize the content, improve our products and services, protect our and your rights, and comply with laws and regulations.*

We may use your personal information to send you promotional information and updates regarding UserVoice and its products and services. You may choose not to receive such information and opt-out of such future communications. All such communications sent to you will also contain instructions for opting-out.

The information that we collect from you may be used in aggregate form in various ways to optimize and improve UserVoice Services. While such information may be based on information about you, it will not identify you personally. We may use such

[80] UserVoice, About us, URL: https://www.uservoice.com/about/
[81] UserVoice, How Microsoft Intune and System Center Configuration Manager take product feedback from concept to release and beyond, URL: https://www.uservoice.com/case-studies/microsoft-intune/
[82] Idem.
[83] Ibid.
[84] Ibid.
[85] UserVoice, Privacy Policy, Effective as of December 9, 2019, URL: https://www.uservoice.com/privacy/

information for the following purposes: website management, administration and security, promotional activities, and research and analysis."[86]

UserVoice describes that it acts as a processor as well as a controller for third parties (in this case: Microsoft), but that it at the same time also analyses the obtained data as a controller for its own purposes:

"*We offer a product to companies that allows them to collect and analyze product feedback provided by individuals who may reside in the EU. In this case, through our contract with the company who is our customer, we are acting as a data processor. We collect, store, and retrieve data on their behalf and at their request.*

We also use our own product to collect, store, and retrieve data to analyze our own product. In this capacity, we are both a data controller and data processor, since the data processing is happening for our own purposes."[87]

UserVoice also writes: "*When acting in our role as a data processor, it is the obligation of the data controller (our customer, a company) to ensure that they have collected consent and made clear that personal data is being collected for the purposes served by the UserVoice platform."*

UserVoice makes a standard Data Processing Addendum available to business customers such as Microsoft.[88] This states that UserVoice processes the data for the purpose of providing the service as described in the Services Agreement.[89]

UserVoice does not publish a separate Services Agreement, but does publish Terms of Service for Account Holders. In it, UserVoice writes that it only processes the data it receives from its clients ('Account Holder Data) in order to fulfil its obligations, and: "*to generate backend reports, graphs, and other materials for internal use in UserVoice's day-to-day operations of the Service. Notwithstanding the foregoing, "Account Holder Data" does not include non-identifiable aggregate data compiled by UserVoice for purposes of improving, maintaining, and/or optimizing the Service.*"[90] This means that UserVoice may process anonymized data without the aforementioned restrictions.

Information about Microsoft's use of UserVoice is limited and not easily accessible. Only if users dive very deeply into Microsoft's explanation pages by clicking multiple links, they can read that help requests are handled by the external company UserVoice. In an explanation page Microsoft about how users can make comments or suggestions to Microsoft, Microsoft explains:

"*New feature ideas*

UserVoice is the official suggestion box for Microsoft Office. Click the link for the product you wish to leave feedback for below, then search to see if somebody else has already offered that feedback. If they have you can add your own comments and

[86] Idem
[87] Ibid.
[88] UserVoice Data Processing Addendum, 26 March 2018, URL: https://www.UserVoice.com/assets/docs/compliance/UserVoice_Customer_DPA_encrypted_.pdf
[89] Idem, section 5.1, Purposes for which the Personal Data shall be processed: "*UserVoice will Process Personal Data for the purpose of providing the Covered Services described in the Services Agreement.*" See also section 6.1 "*UserVoice will Process the Personal Data on documented instructions from Customer in such manner as is necessary for the provision of Services under the Service Agreement, except as may be required to comply with any legal obligation to which UserVoice is subject.*"
[90] UserVoice, Terms of Service, undated, URL: https://www.uservoice.com/tos/

vote for their suggestion. Votes are a great way for users to indicate how important a particular idea or suggestion is to them.

In a smaller font, below this text is stated: "***Note:*** *UserVoice is a 3rd party site, not owned or controlled by Microsoft.*"[91]

Microsoft communicates in a similarly unclear way about itself and the external company UserVoice on a webpage where a user ends up if he wants to give feedback from Teams or Outlook. He then goes to the page 'microsoftteams.uservoice.com'. The web page explains that you can give feedback directly to the Microsoft Engineering team of Teams, with the name of the project manager. "*Hi there, you've reached the user feedback site for Microsoft Teams. It's managed by our Customer Advocacy Team inside Microsoft Teams Engineering led by Karuana Gatimu.*" In light grey at the top the following warning is displayed: *Microsoft has partnered with UserVoice, a 3rd party service providing public discussion forums for product-specific feedback. By continuing to browse this site you agree to UserVoice's Terms of Use."*[92]

UserVoice relies on the EU-U.S. Privacy Shield for the transfer of personal data. This is also evident from the separate Data Processing Addendum that UserVoice offers to customers.[93]

UserVoice is on Microsoft's list of subprocessors for the Online Services, but Microsoft informs data subjects as if UserVoice were a third party and forces data subjects to agree to UserVoice's own privacy policy. According to UserVoice's own terms and conditions, it behaves both as a processor and as a controller.[94]

Since the domains by.uservoice.com and outlook.uservoice.com are marked as "Default Optional" on the Office 365 global network endpoint list, administrators should be able to centrally block traffic to UserVoice.

2.4 Results access request mobile Office apps

On 22 January 2020, formal access requests were sent to Microsoft for the personal data that Microsoft processes as the controller for the two test accounts. Microsoft responded by email of 26 February 2020, stating that it had not found any personal data. "*We have completed our search of databases within Microsoft for the unique personal information you've provided with your request and did not locate any records of personal data in which Microsoft is the controller*." This seems incorrect, because Microsoft, as a controller, should provide data subjects with access to personal data it processes in this capacity. This includes the collected telemetry data, which almost always constitute personal data.

On February 27th, Privacy Company provided an explanation of the request and explicitly requested the collected telemetry data. The specific identifiers that were used in the research were sent along. In addition, information recorded in security

[91] Microsoft, How do I give feedback on Microsoft Office? URL: https://support.office.com/en-gb/article/how-do-i-give-feedback-on-microsoft-office-2b102d44-b43f-4dd2-9ff4-23cf144cfb11?ui=en-US&rs=en-US&ad=US

[92] https://microsoftteams.uservoice.com/forums/555103-public On the main page there is also a frame with a small print: *The Fine Print: We have partnered with UserVoice, third-party service and your use of the portal and your submission is subject to the UserVoice Terms of Service & Privacy Policy, including license terms. Please do not send any novel or patentable ideas, copyrighted materials, samples or demos for which you do not want to grant a license to Microsoft.*

[93] UserVoice's Data Processing Addendum ("DPA"), 26 March 2018, URL: https://www.uservoice.com/assets/docs/compliance/UserVoice_Customer_DPA_encrypted_.pdf

[94] Microsoft Trust Center, https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3 Version 5 September 2019, with a tab completely right with an overview of processors, with a hyperlink to: https://go.microsoft.com/fwlink/p/?linkid=2096306

logs and data collected by third parties and non-Microsoft domains was requested. Microsoft responded to this request on 3 March 2020, explaining that it had already provided access. Microsoft also writes: "*Toward answering your remaining questions, we clarify that the personal data we provided you excluded the following personal data.*

1. *associated with identifiers that can be shared with multiple users;*
2. *related processor services; or*
3. *captured as non-O365 traffic."*

Microsoft gave the following explanation:
"Identifiers. Not all identifiers mentioned are relevant in the context of a DSR request, and we do not provide personal data associated solely with a device ID since that ID may pertain to multiple users. Alternatively, when you sign into your device with your unique Microsoft account, we are able to make available the personal data collected while using that device with your Microsoft account. We make this data available on our privacy dashboard at https://account.microsoft.com/privacy. We also provide users the ability to view and delete diagnostic data on the device with a valid Microsoft account. Note that one of the examples you provided, User ID, was included in our search.

Processor services. We did not provide any personal data, including security logs, that may be associated with processor services. Users of processor services should contact their IT administrator for additional assistance. We do offer robust tools to help our enterprise customers manage their own Data Subject Requests as described in the Office 365 Data Subject Request Guide.

Third-party apps and services. We did not provide you with personal data that might have been captured by Windows traffic. With regard to other third-party apps and services, can you help us understand what you would be looking for? You specifically mentioned Hockey App. We share with you that Hockey App is a Microsoft processor service, so related information would not have been provided in a controller DSR. You can learn more about how your organisation can execute Data Subjects Rights requests in the GDPR guide for the App Center."[95]

The next day, 4 March 2020, the researchers sent a further explanation, namely that the research devices were only used for the research, that the researchers already had accessed the cloud log files that Microsoft processes as processor, and that there can be no non-Office365 traffic because all the traffic was correctly captured and stored from the tested Office apps, not from other apps, and also completely separate from Windows telemetry. Microsoft has not responded since.

Microsoft did not send a reasoned request for a postponement within the maximum period of 30 days permitted by Article 12(3) GDPR for replying to a request for a review, nor did it give any reasons why it did not respond. Failure to respond is equivalent to a refusal. **Microsoft therefore does not provide data subjects with access to the personal data that it processes as a data controller about the mobile Office apps and the Controller Connected Experiences.** Section 2.5 explains that Microsoft has also not provided access to the telemetry that it collects via Office for the Web.

In sum, sections 2.2 to 2.4 show that the telemetry data from the mobile Office apps are personal data because each event contains a unique device identifier and a timestamp. This information is linked to information about the use of an application, depending on the type of action the user performs. This includes actions such as

[95] Email Microsoft 6 March 2020.

starting an app, retrieving files from SharePoint Online or OneDrive for Business, sending a message in Teams or Outlook, opening a calendar from Outlook, retrieving authentication tokens from the Azure Active Directory, using file preview to view a file or error messages.

Microsoft is able to identify an individual user based on the information in the various events that Microsoft collects and stores for at least 90 days (see Section 10 of this report). Microsoft, as a specialised technology company, should be reasonably able to combine telemetry events about individual users through the unique device identifier and timestamp and thus identify data subjects directly or indirectly.

In 2017, the Dutch Data Protection Authority (AP) assessed that the telemetry data that Microsoft collects through Windows 10 are personal data. During this investigation, Microsoft stated that most telemetry data did not relate to individuals, but to (technical aspects of) the operating system.[96] As explained in section 2.1 of this report, Microsoft now acknowledges in its OST that diagnostic data can contain personal data. Nevertheless, Microsoft's response of 6 March 2020 to the findings on outbound traffic from the mobile Office apps shows that Microsoft may still apply an incorrect definition of personal data.

2.5 Diagnostic data Office for the Web

Like the data collection from the mobile Office apps, the data collection via Office for the Web is not transparent. Microsoft does not inform data subjects and system administrators via its information pages that it collects individual usage information in two ways: via telemetry and via system generated server logs, and what diagnostic data Microsoft collects these ways.

There is no Data Viewer Tool or similar functionality to view the telemetry from Office for the Web. Microsoft writes in its response of 6 March 2020 to the technical findings of this report that it does not intend to offer this kind of inspection functionality for Office for the Web telemetry either, because it only collects telemetry at the 'Requirement/Necessary' level.

Microsoft does not offer a separate option to minimise the telemetry flow from the user's browser when using Office for the Web, as has been the case for mobile Office apps since the autumn of 2019. Microsoft has also indicated in its response of 6 March 2020 that this possibility will not come.

Microsoft writes: *"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)."*[97]

During the investigation, content data were found in telemetry events sent from Word and PowerPoint in Office for the Web. The events contained the following personal data: the file name of the presentation, in combination with the unique identifier of the tenant (the holder of an Enterprise license), a unique user identifier (the UserInfo.Id: The user GUID (Globally Unique Identifier) for a Microsoft

[96] Dutch DPA (Autoriteit Persoonsgegevens) report Windows 10 Home and Pro in Dutch only, p. 101, URL: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/01_onderzoek_microsoft_windows_10_okt_2017.pdf

[97] E-mail from Microsoft of 6 March 2020.

work account[98]), information about the device (name and version of operating system and browser), the pathname of the storage of a file in SharePoint, with a hashed file name, and the name of the user as part of the pathname. Microsoft does not provide an explanation why such content data would be necessary for Microsoft to be able to technically provide the services. In Office 365 ProPlus, Microsoft offers three different telemetry settings: Optional, Required and Neither.[99] These types of content data would logically only be collected if a system administrator consents, i.e. at the Optional level.

2.6 Outgoing traffic to third parties Office for the Web

The intercepted traffic from Office for the Web shows that Microsoft sends personal data to two American companies in two ways: Optimizely and Giphy**.** Microsoft does not publish any information about the processing of personal data by these parties. The investigation shows that system administrators are able to centrally block the traffic to Giphy by blocking the traffic to the network endpoint through a group policy, but this option does not exist for the traffic to Optimizely.

2.6.1 Giphy

When using Teams in Office for the Web, Microsoft sends personal data to the U.S. company Giphy, based in New York with a representative in Hamburg. As explained above, Microsoft sends traffic to Giphy when a user wants to insert an image in a Team conversation. At that moment the data are automatically sent to Giphy, without the user receiving any information or having a choice.

Microsoft writes: "*Giphy receives search queries entered by the user and returns suggested entertaining GIF files for the user to add to their content being prepared. The use of this is entirely optional and there is no Microsoft Online Services data processing outcome involved. The presentation of an optional third party functionality such as Giphy does not mean that the third party is acting as a subprocessor of personal data for Microsoft. In such cases, Microsoft has no role in the processing that occurs.*

Microsoft is working to provide ever greater configurability to admins of Office 365. Giphy is an optional third party experience available to users under Giphy's terms and privacy policy. System administrators have the option to disable use of Giphy in Teams. If Giphy is to be avoided by users, then users need to be instructed to avoid Giphy on the web in a browser, in their native application on mobile platforms, and not only in Microsoft applications. If Giphy is prevented, motivated users may just use Imgur." [100]

Giphy is not on Microsoft's list of subprocessors for Online Services.[101] According to Microsoft this is not necessary, because Giphy is an optional service, that is consciously used by end-users. However, Giphy is not included on the list of Additional Optional Connected Experiences, and the use can therefore not be blocked by centrally disabling the Controller Connected Experiences. Nonetheless, administrators can block outgoing traffic to Giphy with a group policy.

[98] Microsoft, 'Required diagnostic data for Office', URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/required-diagnostic-data
[99] Microsoft Office 365 ProPlus diagnostic data, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/overview-privacy-controls
[100] E-mail from Microsoft of 6 March 2020
[101] Microsoft Trust Center, https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3 Version 5 September 2019, with a tab completely right with an overview of processors, with a hyperlink to: https://go.microsoft.com/fwlink/p/?linkid=2096306

2.6.2 *Optimizely*

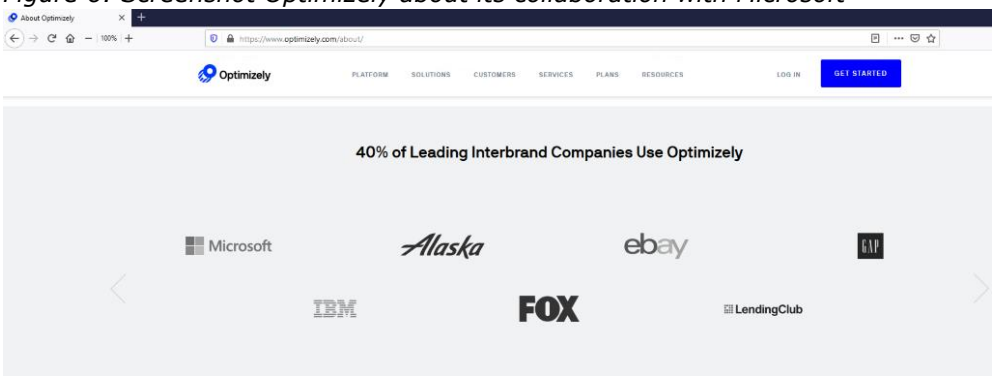
Traffic, including personal data, was sent to San Francisco-based Optimizely[102] during the use of Office for the Web, when visiting OneDrive's website to log in. Through this traffic personal data was sent to the domains cdn.optimizely.com and logx.optimizely.com (including account id, a number of pseudonymized identifiers and a timestamp).

Visiting this website is necessary if people want to view their files stored in OneDrive, because if they work from a browser, they do not have an explorer like Windows 10. Optimizely describes itself as "*the world's leading experimentation platform, empowering marketing and product teams to test, learn and deploy winning digital experiences, every time.*"[103]

A Dutch market research agency summarises Optimizely's processing objectives as follows: "*In addition to A/B testing, Optimizely allows you to test multiple variations and create different visitor segments to be tested. Of course you can also test on mobile devices. Optimizely has a simplified URL pattern and supports A/B testing for iOS applications. In contrast to Google Optimize 360, Optimizely does look at the number of visitors who participate in the test.*"[104]

Optimizely mentions the collaboration with Microsoft on its homepage.

Figure 6: Screenshot Optimizely about its collaboration with Microsoft [105]



According to its privacy statement, Optimizely processes the collected data for several purposes. The purposes highlighted in grey by Privacy Company are the purposes which have something to do with marketing, advertising and profiling.

- *Process your orders and requests and respond to your questions and concerns; for example, if you inquire about our services or submit an application to Optimizely, we may use your data to respond to and process these requests;*
- *provide you with products and services, and personalize your experience; for example, we may use information on your prior activities or job function to tailor the features and content on the Optimizely Services or Sites, or we may use technical data to remember your preferences;*
- *communicate with you about your account or transactions, and provide you with product-related communications, such as information about new features and policy updates;*

[102] Optimizely Privacy Policy, last revised 1 January 2020, URL: https://www.optimizely.com/privacy/ Optimizely, Inc. 631 Howard Street, Suite 100 San Francisco, CA 94105
[103] Optimizely, URL: https://www.optimizely.com/homepage/
[104] Traffic Builders, URL: https://www.traffic-builders.com/tools/wat-is-optimizely/
[105] Screen shot made 31 January 2020, URL: https://www.optimizely.com/about/

- *operate, maintain, analyze, develop, update and improve our Sites, the Optimizely Service, and other products and services we offer. For example, we may administer and track users' activities on our Sites and the Optimizely Service to determine how to improve our content and features, or we may analyze trends and gather demographic information about our user base to better tailor our marketing efforts;*
- *detect, investigate and prevent activities that may violate our policies, including our Acceptable Use Policy, or applicable laws (such as fraud detection and prevention) or that may threaten the security, integrity or availability of our or another party's products, systems and services;*
- *send you news, updates, promotions, product information, event announcements, and other marketing communications. Please see the section entitled "Your Controls and Choices" for an explanation of your choices relating to these communications;*
- *provide you with and target advertising based on your activity and interests, both on our own Sites and applications and on third-party sites and applications;*
- *act pursuant to your consent for a specific purpose not listed in this policy. For example, with your consent, we may post your testimonial along with your name on our Sites. If you wish to update or delete your testimonial, please contact us as explained below; and*
- *perform the activities described in our Cookie Policy."*[106]

Optimizely processes unique user and device identifiers from the traffic from the OneDrive login page and with that, personal data of users of Office for the Web.

Microsoft writes: " *Microsoft's incorporation of services from Optimizely is an example of data traffic that contains neither personal data nor Customer Data. Optimizely is a contemporary webservice available to web property developers like Microsoft, but we are doing so in deliberate ways. For example, Optimizely is used prior to any sign in with organisational credentials on the OneDrive for Business web page, but is not used after such sign in.*

Microsoft has no plans to cease building the type of modern experiences users have come to expect from contemporary web and mobile applications."[107]

Optimizely is not on the list of subprocessors of Microsoft for the Online Services.[108] According to Microsoft, this would not be necessary, because Optimizely does not process personal data (or not anymore) after users have logged in with their school or work account on the web page they visit to use OneDrive.

Microsoft writes in its response of 6 March 2020: "*Microsoft uses internal software logic to enforce that when data processing is performed with Office 365 organisational credentials that any subprocessing of personal data and customer content is limited to the disclosed subprocessors. (Office 365 organisational credentials are often described in our user interface as "Work or School accounts").*"

This is not convincing, as the observed traffic clearly includes personal data. Furthermore, if the traffic to Optimizely is indeed a critical step in the log in process,

[106] Optimizely Privacy Policy, 3. How We Use Information.
[107] Response Microsoft of 6 March 2020.
[108] Microsoft Trust Center, https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3 Version 5 September 2019, with a tab completely right with an overview of processors, with a hyperlink to: https://go.microsoft.com/fwlink/p/?linkid=2096306

and thus essential to gaining access to the Online Service, the processing of data should fall under the data protection arrangements applicable to the Online Services.

2.7 Results access requests Office for the Web

System administrators can obtain access to user's personal data in the audit logs. Microsoft offers a structured query via its DSAR solution, but admins may also perform a self-defined query on the audit logs. Both tools were used.

Data Subject Access Request Tool

The administrator of the test environment has executed an automated access request for the two test accounts of (Privacy Company) employees. Microsoft offers an automated solution for such access since April 2018, the Data Subject Access Request (DSAR) tool.[109]

Through this tool, Microsoft provides administrators with access to the diagnostic data it processes about the use of the Connected Cloud Services SharePoint Online, OneDrive for Business and Exchange Online. This is done via a Content Search in the Security & Compliance Center. This way, the administrators search both content that is still present on Microsoft's cloud servers and the system-generated log files on Microsoft's cloud servers.

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

Microsoft explains:

"*IT admins can use the audit log search tool in the Security & Compliance Center to identity documents, files, and other Office 365 resources that users have created, accessed, changed, or deleted. Searching for this kind activity can be useful in DSR investigations. For example, in SharePoint Online and OneDrive for Business, auditing events are logged when users perform these activities:*

Accessed a file
Modified a file
Moved a file
Uploaded or downloaded a file

You can search the audit log for specific activities, types of activities, activities performed by a specific user, and other search criteria. In addition to SharePoint Online and OneDrive for Business activities, you can also search for activities in Flow, Power BI, and Microsoft Teams. Note that auditing records are retained for 90 days. Therefore, you won't be able to search for user activities that occurred more than 90 days ago. For a complete list of audited activities and how to search the audit log, see Search the audit log in the Office 365 Security & Compliance Center." [110]

Microsoft recommends system administrators to create a separate query per request of a data subject.

[109] Microsoft Blog, Nick Robinson, Introducing Data Privacy in Security & Compliance Center including Data Subject Requests experience, 17 April 2018, URL: https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Introducing-Data-Privacy-in-Security-amp-Compliance-Center/ba-p/183648

[110] Microsoft, Office 365 Data Subject Requests for the GDPR, Use the Office 365 audit log search tool in DSR investigations, 6 April 2019, URL: https://docs.microsoft.com/nl-nl/microsoft-365/compliance/gdpr-dsr-office365?toc=/microsoft-365/enterprise/toc.json

"When you create a new case and start the search, these content locations are searched:
All mailboxes in your organisation (including the mailboxes associated with all Microsoft Teams and Office 365 Groups)
All SharePoint Online sites and OneDrive for Business accounts in your organisation
All Microsoft Teams sites and Office 365 group sites in your organisation
All public folders in Exchange Online."[111]

The result of this DSR consists 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 has for example registered that investigator Floor Terra (owner of one of the two test accounts used by Privacy Company) opened a Word document from SharePoint with the name 'Inzageverzoek_bestemd_voor_testscenarios.doc'.

ExportItem Id	2dc29014-2a9c-475b-9e60-dd5aaa64a3ee
Item Identity	https://XXX-my.sharepoint.com/personal/f_f_terra_XXX_nl/Documents/inzageverzoek_bestemd_voor_testscenarios.docx
Document ID	17650945745221
Selected	Empty
Duplicate to Item	Empty
Original Path	https://XXX-my.sharepoint.com/personal/f_f_terra_XXX_nl/Documents/inzageverzoek_bestemd_voor_testscenarios.docx
Location	https://XXX-my.sharepoint.com/personal/f_f_terra_XXX_nl/
Location Name	Empty
Target Path	Empty
Document Path	https://XXX-my.sharepoint.com/personal/f_f_terra_XXX_nl/Documents/inzageverzoek_bestemd_voor_testscenarios.docx
Subject or Title	inzageverzoek_bestemd_voor_testscenarios
Sender or Created by	Terra, F. Floor
Recipients in To line	Empty
Recipients in Cc line	Empty
Recipients in Bcc line	Empty

[111] Microsoft, Manage GDPR data subject requests with the DSR case tool in the Security & Compliance Center, 25 May 2018, URL: https://docs.microsoft.com/nl-nl/office365/securitycompliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool?redirectSourcePath=%252farticle%252fmanage-dsr-cases-in-the-office-365-security-compliance-center-ce9eb942-3589-42cb-88fd-1576ecb09c5c

To – Expanded	Empty
CC – Expanded	Empty
BCC – Expanded	Empty
DG Expansion Result	Empty
Sent	Empty
Has Attachments	UNTRUE
Importance	Empty
Is Read	UNTRUE
Modified by	Floor Terra
Type	Unknown
Received or Created	1/20/2020 10:37:22 AM
Modified Date	9/12/2019 7:22:00 PM
Size (KB)	21.558
Decode Status	Empty
Compliance Tag	Empty
Summary	"FG Ministerie van Data Bezuidenhoutseweg 73 2594 AC, Den Haag <ddd/> Onderwerp: informatie over mijn persoonsgegevens Geachte heer, mevrouw <ddd/> Concreet wil ik graag weten of u mijn <ddd/>"
Preservation Original Url.	Empty

The results of this Data Subject Request show that Microsoft, via its own system-generated logs with diagnostic data about the use of Office for the Web with the connected cloud storage services, **collects content data from file- and path names of files, and the headers of email.**[112] Because these are online processing operations that take place anyway on Microsoft's cloud servers, Microsoft also 'processes' the contents of files, chats and emails.

Microsoft does not provide information about two data streams via this automated Data Subject Request tool: about the telemetry it collects from Office for the Web and about the use of the Connected Experiences. Microsoft does not provide any information about the Office for the Web applications, nor an overview of all processed unique device / browser and user identifiers.

The results of the access request are personal data, because the log files contain directly identifying data such as name, user name and email address. Microsoft acknowledges this, because it has provided (the administrator of) Privacy Company access as referred to in article 15 of the GDPR. This shows that Microsoft is able to link the user's email address to the user's user name, and to specific actions in the online services Teams, Exchange Online, SharePoint Online and OneDrive for Business.[113]

The results of this automated access request do not give a complete picture of the personal data that Microsoft processes in its system-generated server logs about the

[112] 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 number of 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.
[113] Dutch DPA, research Windows 10, p. 103.

individual use of the Connected Cloud Services SharePoint Online, Exchange Online and OneDrive for Business. Some of these data can however be made visible via the Search-UnifiedAuditlog.[114]

Self-defined query audit logs
Administrators can also write their own queries to search for personal data in the audit logfile. Through a Search Content query administrators can access these logs which register access to the class of data Microsoft defines as Customer Data, both by the users of the software and by Microsoft employees. This includes the logs created by the use of Exchange Online, SharePoint Online en OneDrive for Business.[115]

On 5 February 2020 a query was performed on the audit logs of the diagnostic data that Microsoft stored about the individual usage by the two test accounts of SharePoint Online, Exchange Online and OneDrive for Business. Each "operation" shown in the audit log contains a json object with log data.

The following fields appear in each event:

1. UserType
2. UserKey
3. RecordType
4. Id
5. UserId
6. Version
7. OrganisationId
8. Workload
9. Operation
10. CreationTime
11. ObjectId

Other events occur 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 complete list of events and identifiers found in the audit log is included in Appendix 1 to this report.

From these log files about the two different test users, it can be concluded that a directly identifiable person performed an action at a specific time in one of the five tested apps, 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

[114] Microsoft, Search-UnifiedAuditLog, URL: https://docs.microsoft.com/en-gb/powershell/module/exchange/policy-and-compliance-audit/search-unifiedauditlog?view=exchange-ps
[115] 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 8 July 2019). 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.*"

authenticated. The users are directly identifiable by the fields with the user name 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.

2.8 Diagnostic data Connected Experiences

Since the autumn of 2019, Microsoft offers system administrators an option to centrally ban the use of the four different types of Connected Experiences. Unlike the mobile Office apps, system administrators can only disable the (fourth) group of Additional Optional Connected Experiences in Office for the Web.

The intercepted telemetry events from the outgoing traffic do not contain any data about the use of the Connected Experiences in the mobile Office apps at all. This corresponds to the selected test environment setting to centrally block all Connected Experiences. This blocking however did not function in Outlook and Teams, because there it was still possible to use Connected Experiences such as the Additional Optional Connected Experience Store for Add-ins (for which Microsoft is a controller) and Explanations (the open text field 'Show me what you want to do', which is a Processor Connected Experience).

It is not possible to centrally block the use of all Connected Experiences in Office for the Web. Currently, it is only possible to centrally block the use of the Additional Optional Connected Experiences. See figures 8, 9 and 10 in section 3.1 of this report. The researchers have used as many available Connected Experiences as possible (see the list of available Connected Experiences in section 1.1 of this report). However, the results of the access request do not contain any data about the use of the Connected Experiences in Office for the Web. The executed scenarios are described in **Appendix 2** to this report.

The data collection via the Connected Experiences is not transparent. Microsoft has published information pages on the various types of Connected Experiences (for which Microsoft acts as processor or controller) since May 2019, but does not provide any information about the data it collects as controller when using Office for the Web and the mobile Office apps, either via telemetry events or on its own cloud servers via system generated logs. Microsoft only writes that there are Connected Experiences that analyse content, but not how it handles this data.

Microsoft writes for example:
Connected experiences that analyze your content
Connected experiences that analyze your content are experiences that use your Office content to provide you with design recommendations, editing suggestions, data insights, and similar features. For example, PowerPoint Designer or Editor in Word.[116]
Every mentioned service in the table beneath this explanation is clickable. The link to the Editor (the spelling checker) gives the following information:

"*Editor provides enhanced proofing tools for Office 365 subscribers. Behind the scenes, intelligent services identify spelling, grammar, and stylistic issues, and the Editor pane helps you understand suggestions so you can make choices that improve your writing.*"[117]

[116] Microsoft, Connected experiences in Office, 12 February 2020, URL: https://docs.microsoft.com/nl-nl/deployoffice/privacy/connected-experiences#connected-experiences-that-analyze-your-content
[117] Microsoft, Editor is your writing assistant in Word, URL: https://support.office.com/en-gb/article/editor-is-your-writing-assistant-in-word-91ecbe1b-d021-4e9e-a82e-abc4cd7163d7?ui=en-US&rs=en-GB&ad=GB Via this link, more general information is available about the

Microsoft does not provide any information about the telemetry it collects through the various Connected Experiences. Under the heading "Example of required service data for a connected experience," Microsoft explains that it collects the following data when a user uses the Connected Experience PowerPoint Designer:

"*The required service data that is sent to Microsoft to enable this connected experience for you could include the following:*

- *Customer content, such as the text or images you added to your slide.*
- *Functional data, such as which slide you are working on and its layout.*
- *Service diagnostic data, such as events that tell us if the design idea was correctly applied to your slide and that the service calls were performing correctly*."

Microsoft only mentions five examples of events that are stored on the individual's device as a result of the use of this particular Connected Experience and sent to Microsoft.[118]

Administrators cannot disable this category of service events at all. Microsoft does not provide an overview of the diagnostic data generated in the system log files of the Microsoft servers that offer the Connected Experiences. Nor do the audit log files and automated access requests contain any information about the diagnostic data collected through the Connected Services. Although Microsoft wrote in September 2019 that it hoped to make further privacy improvements in the coming months, it is not clear whether this will also lead to more access to, and public documentation about, the various Connected Experiences.

2.9 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 three types of analytical services as well. With MyAnalytics and Delve, Microsoft analyses data about individual work behaviour. Microsoft makes the insights obtained available to each employee, but not to the administrator (admin). Microsoft describes the services as follows: "*MyAnalytics provides statistics to users to help them understand how they spend their time at work*".[119] Microsoft explains further: "*See how you spent your time over the past month, productivity insights about your work habits, helpful suggestions for improvement, and information about your network, top collaborators, and collaboration activities*." [120]

Through MyAnalytics, an employee not only gains insight into how much time he or she has spent on emails and meetings, but also how many hours someone has worked with specific, named colleagues. In addition, MyAnalytics can show whether a recipient has opened the email. "*In a few cases, MyAnalytics provides people with de-identified information on other people that would not have otherwise been available to them, such as for Email read rates.*"[121]

spelling check options in Word, URL: https://support.office.com/en-gb/article/check-spelling-grammar-and-clarity-0f43bf32-ccde-40c5-b16a-c6a282c0d251

[118] Microsoft, examples of events for service diagnostic data, 10 November 2019, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/required-service-data#examples-of-events-for-service-diagnostic-data

[119] 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

[120] Idem.

[121] Microsoft, MyAnalytics privacy guide, URL: https://docs.microsoft.com/en-gb/workplace-analytics/myanalytics/overview/privacy-guide#myanalytics-vs-workplace-analytics-delve-and-microsoft-graph

Microsoft explains that the MyAnalytics service is executed in the user's inbox on Exchange Online: "***MyAnalytics data is processed and stored in the employee's Exchange Online mailbox****. MyAnalytics processes data from these sources: Exchange Online email and calendar data, chat and call signals from Skype for Business and from Teams, and-if both the organisation's IT administrator and an individual opt in-Windows 10 application activity history. MyAnalytics stores and processes this data inside each employee's Exchange Online mailbox.*"[122]

Microsoft writes about Office Delve: "The brains behind Delve is the Office Graph. The Office Graph continuously collects and analyses *signals that you and your colleagues send when you work in Office 365. For example, when you and a colleague modify or view the same document, it's a signal that you're likely to be working together. Other signals are who you communicate with through email, and who you've shared with, who your manager is, and who has the same manager as you.*"[123] Delve is based on the use of SharePoint Online and OneDrive for Business.

The third analytical service Microsoft offers is Workplace Analytics. This processing is based on the use of email and the calendar, plus additional data that an employer can upload himself. According to Microsoft, Workplace Analytics does not contain identifiable data: "*By default, Workplace Analytics does not show email addresses or other information from Office 365 that directly identifies an individual in any in-product dashboard or query result. However, it does show information from the organisational dataset that your organisation provides for analysis. Thus, if you upload organisational data that includes personal data (for example, employee names and identification numbers), that personal data will appear in in-product dashboards and query results.*"[124]

Microsoft explains that it generally processes pseudonymised data via Workplace Analytics: "*Workplace Analytics automatically replaces email addresses with pseudonyms (cryptographically obscured strings of numbers and letters) in the Office 365 collaboration data that you choose to include for analysis. Using pseudonyms can reduce the likelihood that you will identify a specific person, but the risk of identification remains.*"[125]

Based on the definition in Article 4(5) of the GDPR, pseudonymised data are personal data. Employers are able to analyse individual work patterns based on Workplace Analytics and thus take decisions about the productivity and commitment of an individual employee.

The fourth analytical service offered by Microsoft is Activity Reports in the Microsoft 365 admin center Microsoft enables administrators to create detailed reports on all

[122] Microsoft, MyAnalytics vs. Workplace Analytics, Delve, and the Microsoft Graph, URL: https://docs.microsoft.com/en-gb/workplace-analytics/myanalytics/overview/privacy-guide#myanalytics-vs-workplace-analytics-delve-and-the-microsoft-graph. Also see: Microsoft, Announcement: Create better work habits with MyAnalytics (formerly Delve Analytics), URL: https://techcommunity.microsoft.com/t5/MyAnalytics/Announcement-Create-better-work-habits-with-MyAnalytics-formerly/td-p/15582.

[123] Microsoft, MyAnalytics vs. Workplace Analytics, Delve, and the Microsoft Graph, URL: https://docs.microsoft.com/en-gb/workplace-analytics/myanalytics/overview/privacy-guide#myanalytics-vs-workplace-analytics-delve-and-the-microsoft-graph Also see: Microsoft, Announcement: Create better work habits with MyAnalytics (formerly Delve Analytics), URL: https://techcommunity.microsoft.com/t5/MyAnalytics/Announcement-Create-better-work-habits-with-MyAnalytics-formerly/td-p/15582 .

[124] Microsoft, Types of data for analysis in Workplace Analytics, 2 December 2019, URL: https://docs.microsoft.com/en-gb/workplace-analytics/privacy/data-protection-considerations

[125] Ibid.

kinds of activities per user, such as email behaviour, use of the email app, Skype, Yammer, Teams and activity in OneDrive and SharePoint Online.[126]

Therefore, the four analytical services developed by Microsoft based on the diagnostic data about the use of the Office 365 Connected Cloud Services are a good illustration that the diagnostic data processed by Microsoft through its own server-generated event logs are personal data.

2.10 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.

2.10.1 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 Microsoft 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

Dutch government employees will, depending on the capacity in which they work, often process Classified Information. The Dutch government defines 4 classes of Classified Information, ranging from confidential within the ministry to extra secret state secret.[127]

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, whether or not it qualifies as personal data, must be protected by special safeguards. The processing of this information when related to an individual, can also have a privacy impact. If the personal data of an employee, such as an Enterprise account ID, or unique device identifier, can be connected to the information that this person works with Classified Information, the impact on the private life of this employee may be higher than if that person would only process 'regular' personal 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

[126] Microsoft, Activity Reports in the Microsoft 365 Admin Center, 2 March 2020, URL: https://docs.microsoft.com/en-gb/office365/admin/activity-reports/activity-reports?view=o365-worldwide

[127] 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 paragraph 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 a government employee from effective communication, blackmailing, discrimination, exclusion, identity and/or financial fraud and even a risk of stalking. Government employees 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 Workplace Analytics and the Activity Reports in the Microsoft 365 admin center provide very detailed insights in the behaviour of groups of employees. Although Microsoft aims to provide pseudonymised insights relating to five people or more, Microsoft also warns that individual employees may still be identifiable (such as the director).

It is likely that many government employees process personal data of a sensitive nature with the different products and services included in the Office 365 license on a daily basis. For example, the employees of the tax authority use the Office software. Employees from different ministries may also process sensitive financial data in relation to scholarships or licenses. Employees from the High Councils of State and Advisory Commissions are likely to process sensitive personal data from individual requests and complaints from people in the Netherlands.

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 use of Connected Experiences or in diagnostic data about the opening or saving of files in SharePoint Online or OneDrive for Business. As explained in paragraph 1.1, Microsoft distinguishes between Processor Connected Experiences and Controller Connected Experiences. As explained in paragraph 1.1

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.[128]

Since government organisations such as the police and the judiciary work with the Office software, it cannot be excluded that the diagnostic data may contain information on crimes and convictions in the file and pathnames.

2.10.2 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, contact persons and miscellaneous. Microsofts appendix to the SCC also contains a list of possible data subjects. Government organisations can compare this list with the overview of data subjects in their data processing inventory.

Employees

The government users of the Office software are employees, contractors and (temporary) workers of a governmental organisation.

Their names and other personal information are processed in connection with the documents they create and store in an online storage usually carrying their (last) name, be it Word, Excel, PowerPoint, or another file format. Their names and other personal information are also attached to the emails they send and receive.

Apart from the information generated by the employees themselves, employees are also data subjects in information generated by others. For instance, employees in the cc or bcc field of an e-mail.

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

Contact persons

Information processed with the Office applications is often shared internally and externally. To the extent that diagnostic data contain information about the senders and recipients of particularly emails, this may include data about citizens (customers, clients, patients etc) and collaborators. Diagnostic data may include the sender's name and email address, as well as the time when an email was sent or received.

Dutch citizens and other data subjects

Besides employees and the group of people who are directly in touch with employees, there is a third miscellaneous group of individuals whose personal data may be processed in snippets of content included in the diagnostic data generated by the use of the Office software. The diagnostic data could also include information about the communications pattern of people that do not work for the Dutch government, but are allowed to use the Office software. For example, in penitentiary facilities, detainees can use Office products such as Outlook. The fact they exchange confidential information with their lawyers may be included in the diagnostic data. Other examples involve people whose information is forwarded, but who are not directly in touch with the Ministry themselves, or people who apply for a job.

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

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. Data processing

This section discusses the different privacy controls for end-users and administrators to minimise the processing of data about the individual use of Office for the Web, the mobile Office apps and the additional online services in combination with the use of the associated Microsoft cloud services.

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

3.1 Privacy controls system administrators

Telemetry settings

Since the fall of 2019 or since January 2020 (depending on the update regime used by administrators for Office365 updates), Microsoft offers system administrators the ability to minimise the level of diagnostic data traffic in the mobile Excel, PowerPoint and Word apps.

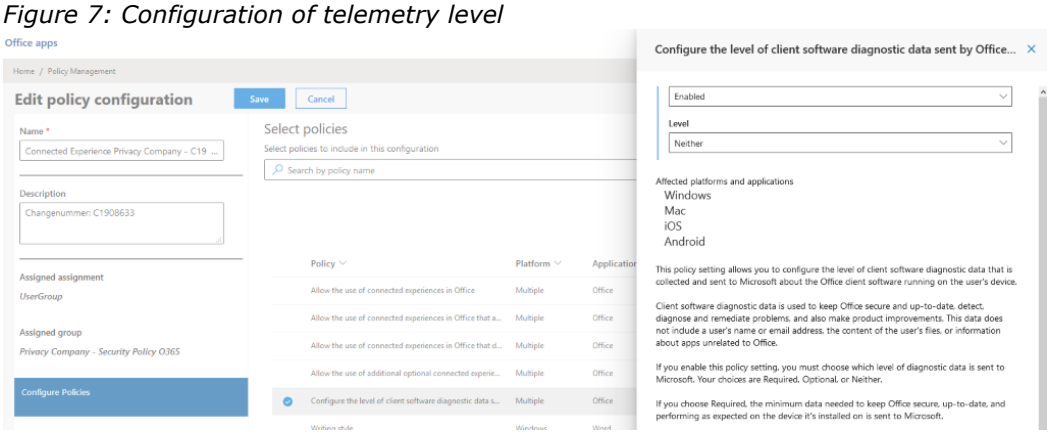
Since the spring of 2019 Microsoft distinguishes between three telemetry levels in the Enterprise versions of Office 365:

a. Optional
b. Required
c. Neither[129]

This privacy control does not exist for the telemetry events from the OneDrive, Outlook and Teams apps and from Office for the Web. See Figure 7 below.

In the test environment the telemetry level for the mobile Office apps was set to the lowest level: 'Neither'.

Figure 7: Configuration of telemetry level



Connected Experiences

[129] Microsoft, Required diagnostic data for Office, 21 February 2020, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/required-diagnostic-data

A second important privacy control for system administrators is to centrally block one or more groups of Connected Experiences. In the mobile Office apps, it is possible to disable all Connected Experiences. When it comes to Office for the Web (Figure 9 below), system administrators can only disable the Additional Optional Connected Experiences, not the other Connected Experiences.

In its new OST of January 2020, Microsoft suggests that administrators can opt-in to the Connected Experiences, while it is an opt-out. *"Additionally, if permitted by Customer, users may elect to use connected services subject to terms of use other than this OST and with respect to which Microsoft is a data controller, as identified in product documentation."*[130]

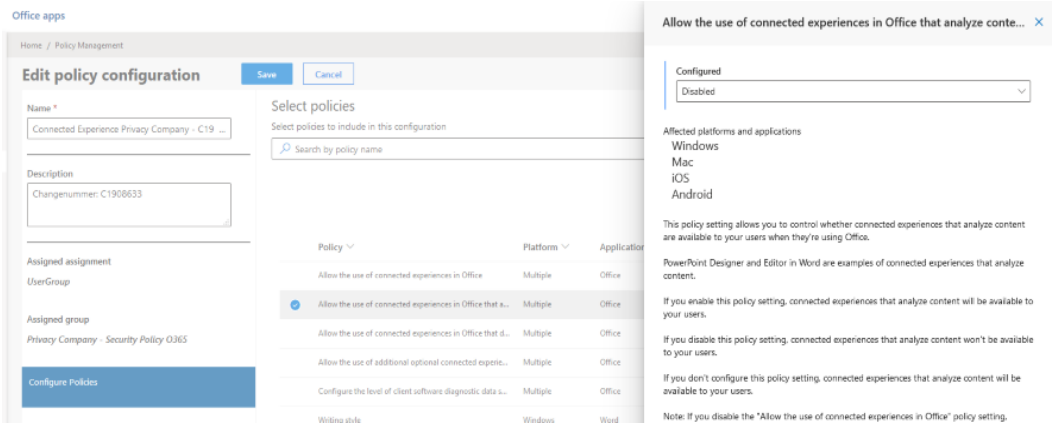
Microsoft explains that system administrators have three controls to disable the four different categories of Connected Experiences for the Word, PowerPoint, Excel and OneNote apps on iOS and Android.[131] There is no separate control for the fourth category of 'other' Connected Experiences.

"If you are an administrator, refer to the following articles for details on how to enable or disable optional connected experiences for your users:

1. *Use preferences to manage privacy controls for Office on iOS devices.*[132]
2. *Use policy settings to manage privacy controls for Office on Android devices.*[133]

If administrators find this selective disablement insufficient, they can also choose to block the use of the mobile Office apps completely. The tests conducted for this DPIA show that it is possible for administrators to centrally block access to the work environment for all work accounts used on (all) mobile Office apps.

Figure 8: Configuration Connected Experiences that process content data



[130] Microsoft OST March 2020, Office 365 Applications, p. 18-19
[131] Microsoft, Overview of optional connected experiences in Office, 14 January 2020, URL: https://docs.microsoft.com/us-en/deployoffice/privacy/optional-connected-experiences
[132] Microsoft, Use preferences to manage privacy controls for Office on iOS devices, URL: https://docs.microsoft.com/nl-nl/deployoffice/privacy/ios-privacy-preferences
[133] Microsoft, Use policy settings to manage privacy controls for Office on Android devices, URL https://docs.microsoft.com/nl-nl/deployoffice/privacy/android-privacy-controls

Figure 9: Configuration Connected Experiences which download content

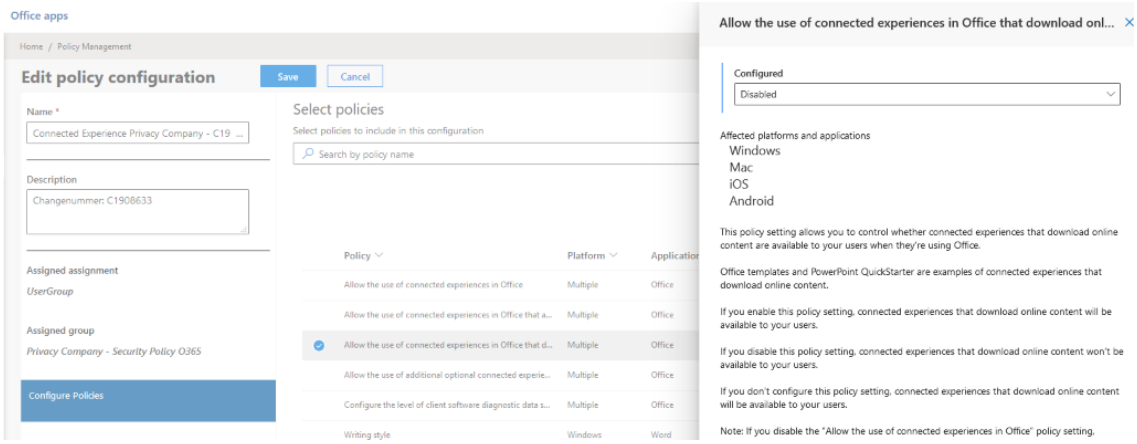
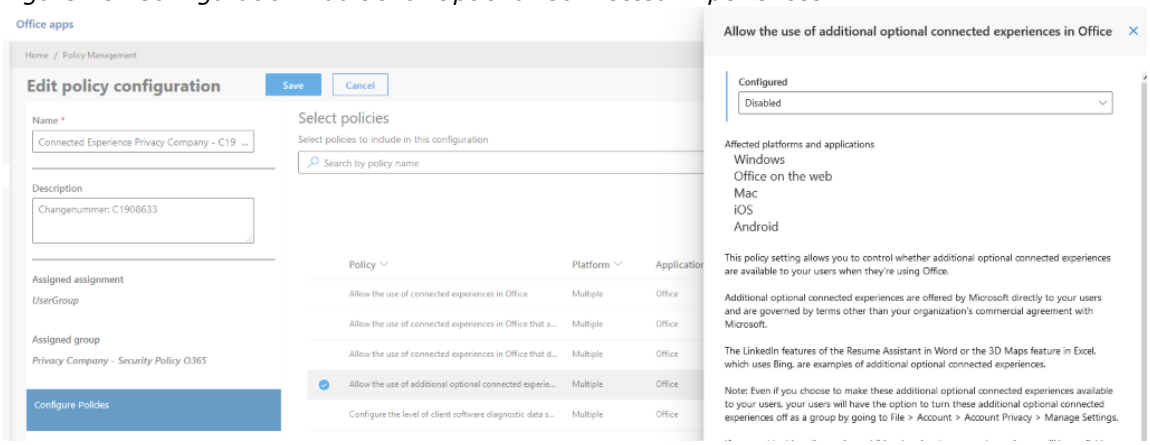


Figure 10: Configuration Additional Optional Connected Experiences



Network endpoints

System administrators are able to centrally prevent traffic to specific network endpoints through a group policy.

Use of add-ins separate from Office Store

Part of the Controller Connected Experiences is (access to) the Office Store. Microsoft enables system administrators to manage add-ins for users themselves, even if those users do not have access to the Office Store.

Microsoft writes: "*As an organisation you may wish to prevent the download of new Office add-ins from the Office Store. This can be used in conjunction with Centralized Deployment to ensure that only organisation-approved add-ins are deployed to users within your organisation.*"[134]

Tests executed for this DPIA show that it is possible for admins to separately offer the use of add-ins such as iWrite, even while all Connected Experiences were centrally switched off for end-users, including access to the Office Store.

[134] Explanation Microsoft how administrators can assign add-ins themselves, URL: https://docs.microsoft.com/en-gb/office365/admin/manage/manage-deployment-of-add-ins?view=o365-worldwide

Figure 11: Admin managed Office Add-ins

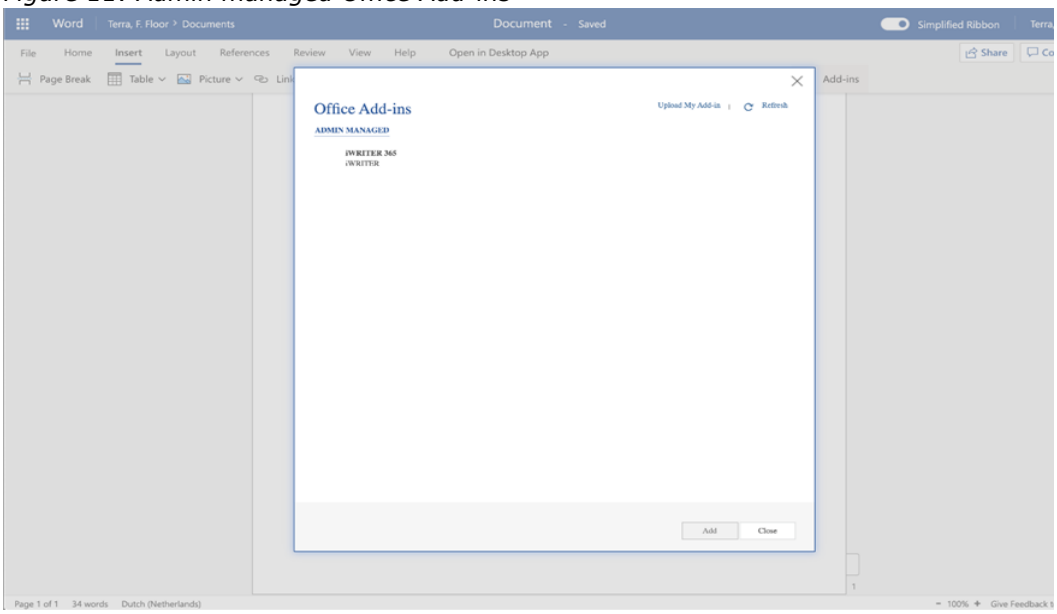
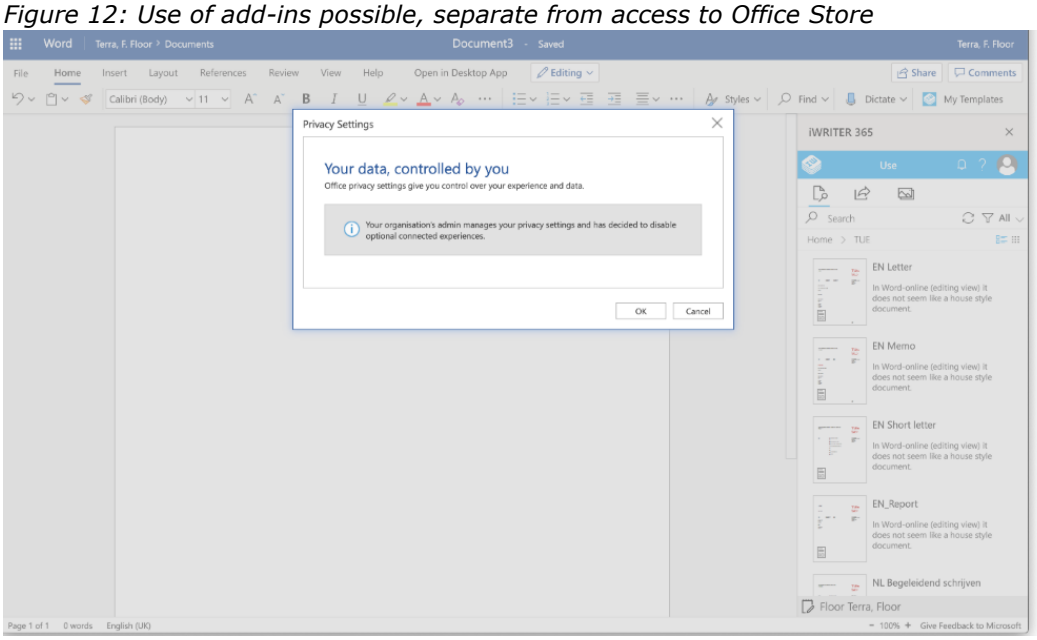


Figure 12: Use of add-ins possible, separate from access to Office Store



3.2 Privacy controls end users

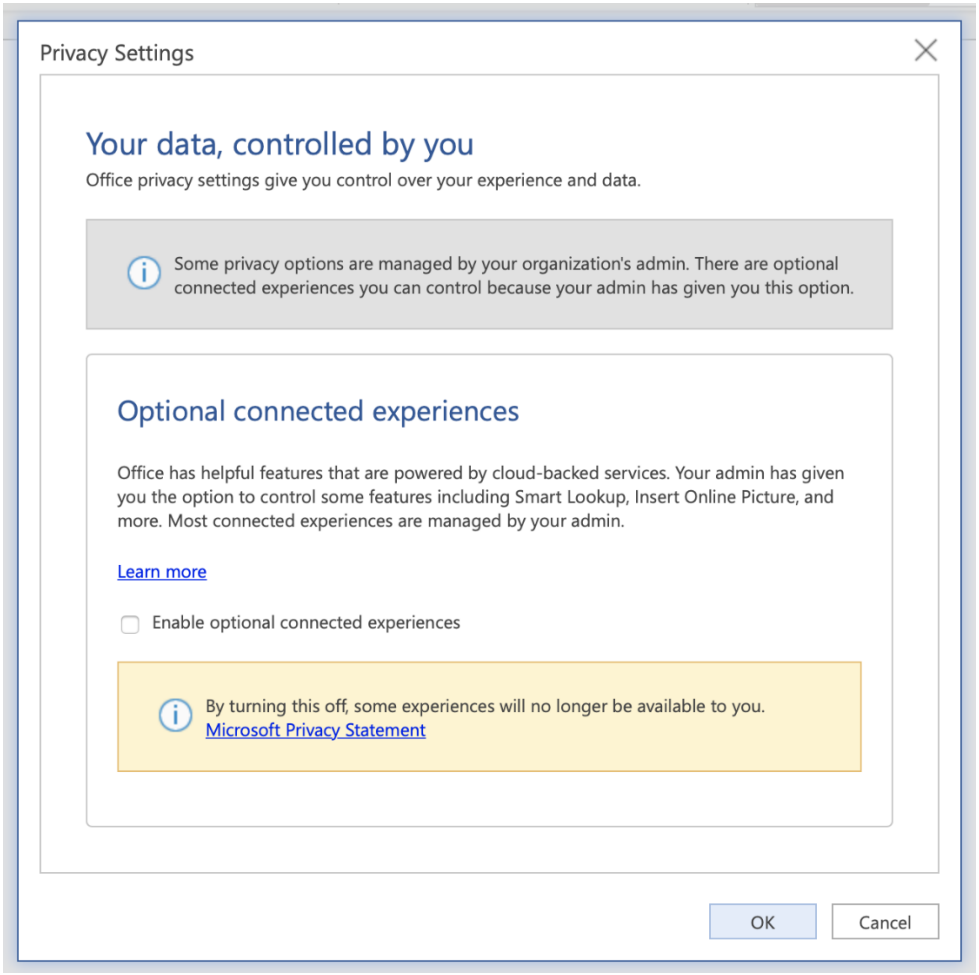
If the system administrator does not centrally block the use of the Connected Experiences, users can also exercise an opt-out in Office for the Web themselves. This option is only available in the Word, PowerPoint and Excel applications, not in the web versions of Outlook, Teams and OneDrive. Microsoft explains: *Office includes these connected experiences. If you'd like to turn these experiences off, go to any Office 365 application - such as Word, Excel, or PowerPoint - and go to* ***File*** *>* ***Account*** *>* ***Manage Settings*** *(In Outlook it's under* ***Office Account****). There you can disable or enable, either category (or both).*[135]

[135] https://support.office.com/en-gb/article/connected-experiences-in-office-8d2c04f7-6428-4e6e-ac58-5828d4da5b7c?ns=IWAPPC&version=16&ui=en-US&rs=en-US&ad=US

The privacy controls for end-users are similarly limited for the mobile Office apps. The possibility to disable the Connected Experiences (if not already blocked by the administrators), and to view the telemetry via the Data Viewer Tool, are currently only available for Word, PowerPoint and Excel, not for the mobile Outlook, Teams and OneDrive apps. The option for telemetry seems to exist in the OneNote app, but the option to view the telemetry data has no functionality yet.

As explained above, Microsoft announced on its Office 365 ProPlus telemetry data information page, that it wanted to extend the improved privacy controls to additional Office clients in the coming months, including Teams and the mobile Office apps.[136]

Figure 13 choices end-users in Office for the Web[137]

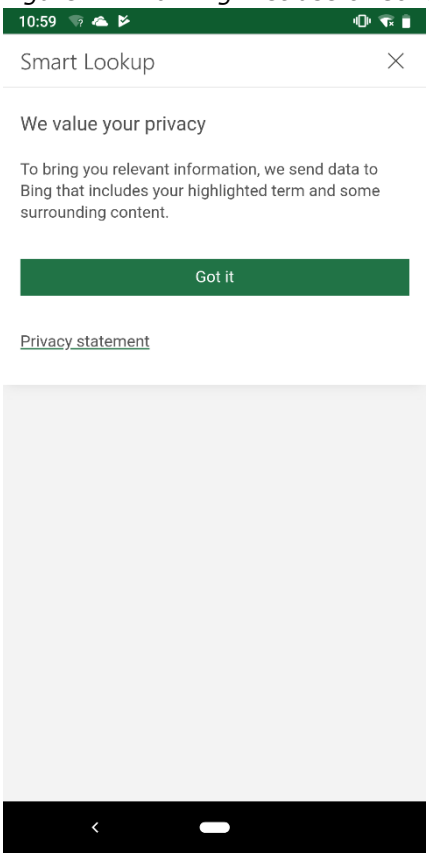


[136] Microsoft Deploy Office, Privacy for Office 365 ProPlus / Overview of privacy controls for Office 365 ProPlus, 9 December 2019, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/overview-privacy-controls

[137] Microsoft writes: "If you are signed in with a work or school account, the admin in your organisation will decide whether these connected experiences are available to you. You won't see any choices for these connected experiences if you go to File > Account > Account Privacy > Manage Settings. If you're using Office for Mac, open any Office application and select the app menu (such as Word, or Excel) > Preferences > Privacy. This will open the Account Privacy settings dialog box where you can see your privacy options." Microsoft, Choose whether these connected experiences are available to use, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/connected-experiences#choose-whether-these-connected-experiences-are-available-to-use

If the system administrators have not prohibited the use of the Controller Connected Experiences, Microsoft will display a Bing-based Connected Experience warning when the Controller Connected Experiences are used for the first time. The warning states that data will be sent to Microsoft. Microsoft informs that it is not only the highlighted search term, but also the information around it. Microsoft also shows a hyperlink to its (general) privacy statement.

Figure 14: warning first use of Controller Connected Experience



Microsoft only shows this warning once in Office for the Web and in the mobile Office apps, without a very clear question for consent. After that, all Connected Experiences are automatically turned on. The user cannot see this, nor can they disable these functions.

Microsoft explains how administrators can block access to these Controller Connected Experiences.

"In addition to the connected experiences mentioned above, there are some optional connected experiences that you may choose to allow your users to access with their organisation account, which is sometimes referred to as a work or school account. For example, Office add-ins that are downloaded through the Office Store to your device. For more examples, see Overview of optional connected experiences in Office.
If you don't set this preference, optional connected experiences are available to users with an Office 365 subscription that are signed in with a work or school account.

Unless you have set this preference to FALSE, these users can choose to turn off optional connected experiences by going to ***Settings > Privacy Settings****."*[138]

There is no possibility for the system administrators to prohibit users from downloading the mobile Office apps unless they only work with fully managed devices. However, the administrators can block access from the mobile Office apps to the work Office environment.

4. Purposes of the processing

Government organisations can use the diagnostic data about Office 365 for security and compliance purposes, for example to detect and mitigate security incidents and to control the access to personal data processed through Office 365. Use of the cloud storage and mail services allows government organisations to offer a reliable service that is accessible from multiple locations. These government 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 Office for the Web and the log files of the Connected Cloud Services, content data from Office for the Web, the Processor Connected Experiences and the Connected Cloud Services;
2. Purposes for the processing of telemetry events from the mobile Office apps and processing content data from the Controller Connected Experiences.

4.1 Purposes Office for the Web, Processor Connected Experiences and the Connected Cloud Services

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 personal data that it processes through the use of Office for the Web and the Connected Cloud Services SharePoint Online, Exchange Online, OneDrive for Business and the Azure AD after a user is signed in with a school or work account.

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 where 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.

Nevertheless, Microsoft appears to be sending personal data to two external companies from the Core Online Service Office for the Web that process the data for marketing and A/B test purposes. This does not correspond to the three authorised purposes**.** Traffic is sent to Optimizely when using OneDrive via Office for the Web

[138] Microsoft, Use preferences to manage privacy controls for Office on iOS devices, 19 October 2019, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/ios-privacy-preferences

and to Giphy when a user wants to insert an image in Teams. As explained in section 2.4 of this report Giphy and Optimizely are not mentioned on the exhaustive list of subprocessors that Microsoft engages for the Core Online Services. Microsoft does not publish any information about the processing of personal data by these parties. In respond to the technical findings in this report Microsoft has answered that the traffic to Giphy is completely optional and that users themselves have to decide whether they want to use this external service. The technical research shows that administrators can centrally block the traffic.

This control is not available for the traffic to Optimizely. According to Microsoft, this traffic only occurs on the web page before a user signs in with his school or work account in order to use OneDrive. Therefore, this traffic would be out of target for the Online Services. In view of Microsoft's position, this data processing is discussed below, in section 4.2 on the purposes of processing when Microsoft is the data controller (and not the processor).

4.2 Purposes mobile Office apps and Controller Connected Experiences

Microsoft links to its general consumer privacy statement for the purposes of the processing of personal data from the mobile Office apps and the Controller Connected Experiences. As explained above, in section 4.1, the privacy guarantees from the OST and the privacy amendment do not apply to traffic from Office for the Web as long as the user has not yet logged in with a work or school account, or use of external services embedded in Office for the Web.

In its privacy policy Microsoft reserves the right to process the personal data it collects for seventeen purposes (see also sections 5.2 of this report). This includes the display of personalised advertising.

The seventeen purposes are:

1. ***Provide our products.*** *We use data to operate our products and provide you with rich, interactive experiences. For example, if you use OneDrive, we process the documents you upload to OneDrive to enable you to retrieve, delete, edit, forward, or otherwise process it, at your direction as part of the service. Or, for example, if you enter a search query in the Bing search engine, we use that query to display search results to you. Additionally, as communications are a feature of various products, programs, and activities, we use data to contact you. For example, we may contact you by phone or email or other means to inform you when a subscription is ending or discuss your licensing account. We also communicate with you to secure our products, for example by letting you know when product updates are available.*
2. ***Product improvement.*** *We use data to continually improve our products, including adding new features or capabilities. For example, we use error reports to improve security features, search queries and clicks in Bing to improve the relevancy of the search results, usage data to determine what new features to prioritize, and voice data to improve speech recognition accuracy.*
3. ***Personalization.*** *Many products include personalized features, such as recommendations that enhance your productivity and enjoyment. These features use automated processes to tailor your product experiences based on the data we have about you, such as inferences we make about you and your use of the product, activities, interests, and location. For example, depending on your settings, if you stream movies in a browser on your Windows device, you may see a recommendation for an app from the Microsoft Store that streams more efficiently. If you have a Microsoft account, with your permission, we can sync your settings on several devices. Many of our products provide controls to disable personalized features.*

4. ***Product activation.*** *We use data—such as device and application type, location, and unique device, application, network, and subscription identifiers—to activate products that require activation.*
5. ***Product development.*** *We use data to develop new products. For example, we use data, often de-identified, to better understand our customers' computing and productivity needs which can shape the development of new products.*
6. ***Customer support.*** *We use data to troubleshoot and diagnose product problems, repair customers' devices, and provide other customer care and support services, including to help us provide, improve, and secure the quality of our products, services, and training, and to investigate security incidents. Call recording data may also be used to authenticate or identify you based on your voice to enable Microsoft to provide support services and investigate security incidents.*
7. ***Help secure and troubleshoot.*** *We use data to help secure and troubleshoot our products. This includes using data to protect the security and safety of our products and customers, detecting malware and malicious activities, troubleshooting performance and compatibility issues to help customers get the most out of their experiences, and notifying customers of updates to our products. This may include using automated systems to detect security and safety issues.*
8. ***Safety.*** *We use data to protect the safety of our products and our customers. Our security features and products can disrupt the operation of malicious software and notify users if malicious software is found on their devices. For example, some of our products, such as Outlook or OneDrive, systematically scan content in an automated manner to identify suspected spam, viruses, abusive actions, or URLs that have been flagged as fraud, phishing, or malware links; and we reserve the right to block delivery of a communication or remove content if it violates our terms.*
9. ***Updates.*** *We use data we collect to develop product updates and security patches. For example, we may use information about your device's capabilities, such as available memory, to provide you a software update or security patch. Updates and patches are intended to maximize your experience with our products, help you protect the privacy and security of your data, provide new features, and ensure your device is ready to process such updates.*
10. ***Promotional communications.*** *We use data we collect to deliver promotional communications. You can sign up for email subscriptions and choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. For information about managing your contact data, email subscriptions, and promotional communications, see the How to access and control your personal data section of this privacy statement.*
11. ***Relevant offers.*** *Microsoft uses data to provide you with relevant and valuable information regarding our products. We analyze data from a variety of sources to predict the information that will be most interesting and relevant to you and deliver such information to you in a variety of ways. For example, we may predict your interest in gaming and communicate with you about new games you may like.*
12. ***Advertising.*** *Microsoft does not use what you say in email, chat, video calls, or voice mail, or your documents, photos, or other personal files to target ads to you. We use data we collect through our interactions with you, through some of our products, and on third-party web properties, for advertising in our products and on third-party properties. We may use automated processes to help make advertising more relevant to you. For more information about how your data is used for advertising, see the Advertising section of this privacy statement.*
13. ***Transacting commerce.*** *We use data to carry out your transactions with us. For example, we process payment information to provide customers with*

product subscriptions and use contact information to deliver goods purchased from the Microsoft Store.

14. ***Reporting and business operations.*** *We use data to analyze our operations and perform business intelligence. This enables us to make informed decisions and report on the performance of our business.*
15. ***Protecting rights and property.*** *We use data to detect and prevent fraud, resolve disputes, enforce agreements, and protect our property. For example, we use data to confirm the validity of software licenses to reduce piracy. We may use automated processes to detect and prevent activities that violate our rights and the rights of others, such as fraud.*
16. ***Legal compliance.*** *We process data to comply with law. For example, we use the age of our customers to ensure we meet our obligations to protect children's privacy. We also process contact information and credentials to help customers exercise their data protection rights.*
17. ***Research.*** *With appropriate technical and organisational measures to safeguard individuals' rights and freedoms, we use data to conduct research, including for public interest and scientific purposes.*

In the section 'Advertising' in the privacy statement, Microsoft explains: "*We may share data we collect with partners, such as Verizon Media, AppNexus, or Facebook (see below), so that the ads you see in our products and their products are more relevant and valuable to you.*"[139]

Microsoft mentions a number of examples of this type of other companies that can get usage data: "*Additionally, Microsoft partners with third-party ad companies to help provide some of our advertising services, and we also allow other third-party ad companies to display advertisements on our sites. These third parties may place cookies on your computer and collect data about your online activities across websites or online services. These companies currently include, but are not limited to: AppNexus, Facebook, Media.net, Outbrain, Taboola and Verizon Media.*"[140]

Microsoft explicitly mentions the possibility that it can base advertisements on usage data. "*The ads that you see may also be selected based on other information learned about you over time using demographic data, location data, search queries, interests and favorites, usage data from our products and sites, and the information we collect about you from the sites and apps of our advertisers and partners. We refer to these ads as "personalized advertising" in this statement.*"[141]

These same seventeen purposes also apply to the processing of personal data that Microsoft processes via its Controller Connected Experiences.[142] Microsoft explains that these services are optional. "*It is important to know that these optional cloud-backed services are not covered by your organisation's license with Microsoft. Instead, they are licensed directly to you. By using these optional cloud-backed services, you also agree to the terms of the Microsoft Services Agreement and privacy statement*."[143] As explained in section 1.1, not all of these services are available in Office for the Web and the mobile Office apps, and there are other Controller Connected Experiences available that are not documented by Microsoft on this list.

[139] Microsoft privacy statement February 2020, Advertising,URL: https://privacy.microsoft.com/nl-nl/privacystatement#mainadvertisingmodule
[140] Ibid.
[141] Ibid.
[142] Microsoft, Deploy Office, Overview of optional connected experiences in Office, 29 February 2020, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/optional-connected-experiences
[143] Ibid.

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.

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 the Dutch government and Microsoft

Under the privacy amendment with the Dutch government, 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.

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 should allow the Dutch government organisations to fulfil their role as data controllers for the diagnostic data relating to the Online Services in compliance with data protection legislation. However, this DPIA shows that Microsoft does not always apply these contractual guarantees. Contrary to the contractual agreement, Microsoft acts as a controller with respect the mobile Office apps and specific transfers of personal data to third parties in Office for the Web, all as further described below.

5.4 Data controller

Pursuant to the privacy amendment with the Dutch government, Microsoft should act as a processor for Office for the Web and personal data received, collected, generated or derived through the use the mobile Office apps with organisational credentials. However, the research for this DPIA has identified that Microsoft does not comply with the privacy amendment and acts as a controller with respect to diagnostics data from Office for the Web (in certain situations) and the mobile Office apps.

Office for the Web

It follows from the technical research that Microsoft does not always factually behave as a processor in Office for the Web. Microsoft forwards personal data to two external companies in Teams and OneDrive in Office for the Web. Giphy is an independent data controller and processes the data for its own marketing purposes. This may also be the case for Optimizely. Their processing operations are likely not limited to the three authorised purposes. According to Microsoft both processing operations fall outside the scope of this purpose limitation because the use of Giphy is voluntary, and Optimizely is only used before a user has logged in. This reasoning is flawed. Microsoft has made these operations possible. In doing so, Microsoft has at least partially determined the purposes for this data processing. The processing cannot be qualified as optional and Microsoft cannot claim it has an independent contract with, or consent from the end users. Users must visit the page with the Optimizely interaction in order to log into their work account for OneDrive. With regard to Giphy, Microsoft does not give users a clear warning that they are going to provide personal data to an external American company if they click on the neutral icon 'insert image' in Teams. As soon as they click, before they can see they have entered the outside domain of Giphy, their IP address, device information and keywords are transferred to Giphy. Only a controller may determine the purposes of the processing. By enabling this processing, Microsoft is behaving as a data controller.

In addition, Microsoft collects personal data and content data via telemetry events from Office for the Web. It is not clear to what extent Microsoft adheres to the authorised three purposes for this processing or even considers itself to be a processor. In its response to the technical findings in this report, Microsoft stated that it *uses internal software logic to enforce that when data processing is performed with Office 365 organisational credentials that any* ***subprocessing of personal data and customer content*** *is limited to the disclosed subprocessors."*[144]

In this explanation, Microsoft explicitly does not mention the term "diagnostic data," by which Microsoft only means the telemetry data. Although Microsoft uses the GDPR definition of personal data in its OST and DPA, and in the privacy amendment with the Dutch government, this explanation leaves too much room for interpretation. It cannot be ruled out that Microsoft considers itself to be an independent data controller for the telemetry data from Office for the Web, because this data flow is separate from the data actively shared via the applications after the users have logged in to their work account.

[144] Email Microsoft of 6 March 2020.

5.4.1 Mobile Office apps

The right to use the mobile Office apps with a work or school account is granted in Microsoft's Online Service Terms. As a result, the data protection terms of the Online Service Terms, the Data Protection Addendum and the privacy amendment apply to the processing of all personal data received, collected, generated or derived through the use of the mobile Office apps with a work or school account. This includes personal data in diagnostic data (including telemetry). It makes no difference whether the diagnostic data relates to the performance of the mobile Office application on the device or the use of the Office application itself. All personal data associated with organisational credentials falls within the scope of the privacy amendment. This means that that Microsoft may only act as a processor, except for the Controller Connected Experiences, certain purposes for which it has a legitimate business interest and in respect of disclosures to authorities.

In response to earlier questions from SLM Microsoft Rijk to Microsoft about the applicability of the OST to the mobile Office apps, Microsoft stated:
"All Office Mobile applications are (indeed) offered under a EULA between Microsoft and the mobile device user, and the diagnostic data it collects is governed under the Microsoft Privacy Policy and the EULA. However, and crucially, data provided to Microsoft or collected by Microsoft through the use of an Azure AD Account authenticated in the Mobile apps are governed under the OST and your agreement."[145]

In response to the technical findings from this report, Microsoft has explicitly confirmed that it acts as data controller for the mobile Office apps. Microsoft writes: "*For Microsoft applications provided to users under our Microsoft Service Agreement and Privacy Policy (such as Office branded applications for mobile platforms, or online services where users authenticate with a Microsoft Account identity), Microsoft declares that third party subprocessing may be occurring. Those applications are contracted with the user, not with the organisation, and Microsoft processes personal data in these applications as a GDPR data controller, except in certain circumstances.*"[146]

Microsoft also writes: "*Throughout the work are several references to the Office Mobile applications being licensed to the organisational customer as part of Office 365 Online Services. This is not the licensing or offer basis for the Office Mobile applications. (.) The software is licensed as to the used and is subject to the contract license provided from the store and subject to the provisions of our privacy policy*."[147]

And: "*Office Mobile Applications are not part of Office 365. (…) These are licensed to users for uses in multiple scenarios*."[148]

And: "*For data processing occurring under organisational credentials relative to Online Services accessible within the mobile Office apps, Microsoft is a processor and acting in accordance with processing instructions.*" [149]

Microsoft's position that the use of the mobile Office apps is not part of Office 365 is untenable. Firstly, because the right to use the mobile Office apps for up to

[145] DPIA Microsoft Office 365 Online and Mobile, SLM Microsoft Rijk 23 July 2019, p. 31, 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
[146] Email Microsoft of 6 March 2020.
[147] Ibid.
[148] Ibid.
[149] Ibid.

five devices per licensed organisational ID is included in the Online Service Terms. Without a license granted under the volume licensing agreement (or another subscription that authorises commercial use), it is not even allowed to use the mobile Office apps for commercial purposes.

Second, Microsoft actively promotes the mobile Office apps as an integral part of Office 365 Enterprise. Upon the introduction of the mobile Office apps in Office 365 Enterprise in the summer of 2018, Microsoft wrote: "*We are also simplifying our licensing to add the Office mobile Office apps for iOS and Android to Office 365 E1, F1, and Business Essential licenses. With this change, all users licensed for Microsoft 365 and Office 365, including Firstline Workers, will be able to use the Office mobile Office apps and be productive on the go. Outlook for iOS and Android is available to users now. Word, PowerPoint, Excel, and OneNote mobile Office apps will be available over the next few months.*"[150]

In Microsoft's publication 'Seize the cloud, 7 reasons to switch to Microsoft 365' from 2019, Microsoft names the mobile Office apps as reason 3 out of 7 (only preceded by the teams and secure file sharing options) to switch to Microsoft 365: '*Office 365 allows teams to stay connected and collaborate on documents from any device with mobile versions of Office apps.*'[151]

That the mobile Office apps are an integral part of the Office 365 offering also follows from the user account page. When a government or student user is logged in to Office 365 ProPlus or uses Office for the Web with a Microsoft work or student account, Microsoft encourages the user to install the mobile Office apps on 5 different tablets and smartphones. See figures 15 and 16 below.

Although the use of the mobile Office apps is clearly part of the Enterprise volume license of the Dutch government, Microsoft maintains its position that the mobile Office apps are a consumer product that Microsoft licenses to the end user and for which it is a controller. Somehow, Microsoft seems to assume that it only has to be a processor in respect of personal data associated with governmental IDs when this is 'relative to the Online Services': "*For data processing occurring under organisational credentials relative to Online Services accessible within the mobile Office apps, Microsoft is a processor and acting in accordance with processing instructions.*" When Microsoft deems processing not relative to the Online Services, Microsoft refers back to the end user agreement and acts as a controller.

This shows that Microsoft operates under the incorrect assumption that it has discretion to process personal data obtained through use of a mobile Office app with organisational credentials as a controller for purposes that have not been authorised by the government organisation, simply by labelling those processings *not* relative to Online Services. This is wrong. The privacy amendment clearly states that Microsoft may only act as a processor. Thus, any functionality or processing outside of the customers instructions must be authorised by the controller, which is the customer and not Microsoft. There is no room for Microsoft to determine additional purposes or to offer additional functionality to end users outside of the government organisation's documented instructions. The only exceptions are the Controller Connected

[150] Microsoft, Making IT simpler with a modern workplace, 27 April 2018, URL: https://www.microsoft.com/en-gb/microsoft-365/blog/2018/04/27/making-it-simpler-with-a-modern-workplace/
[151] Available at https://info.microsoft.com/ww-landing-7-reasons-to-switch-to-microsoft-365-acquisition-ebook.html?LCID=EN-US.

Experiences that have not been disabled by the customer, the processing for Microsoft's own legitimate business purposes (e.g. invoicing) and disclosures to authorities, if Microsoft would be legally prohibited from forwarding the request or order to the customer.

Figure 15. Information that signed-in users can download the apps on 5 devices

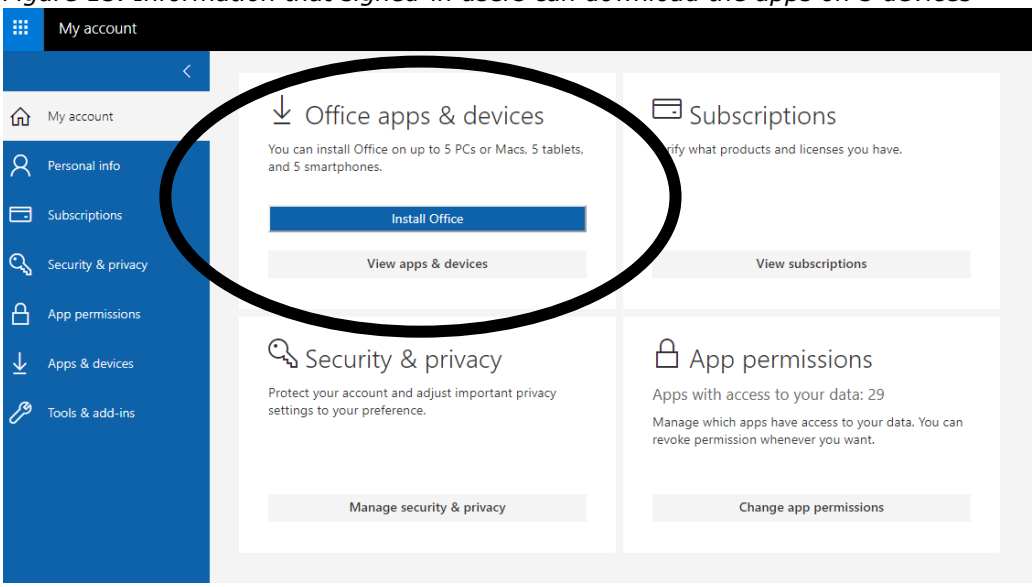
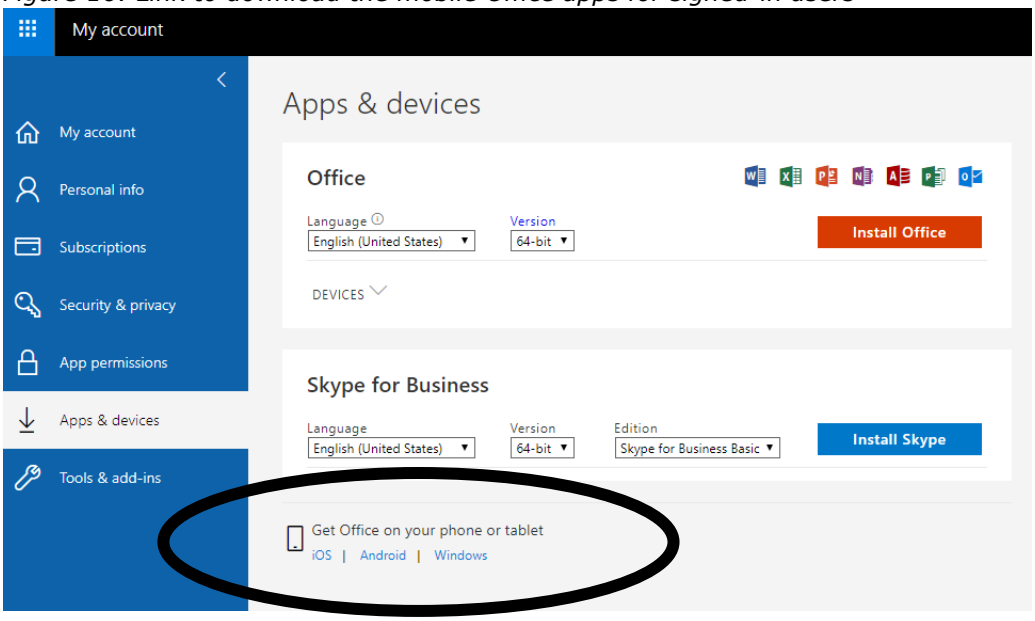


Figure 16: Link to download the mobile Office apps for signed-in users



5.4.2 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 4.2 (*Purposes mobile Office apps and Controller Connected Experiences*) Microsoft explains that these services are optional and refers users to its general privacy statement. In its guidance for administrators on the use of the DSAR tool, Microsoft explains:

"***Optional connected online services**: Office 365 ProPlus makes certain optional connected online services available to the user. The list of services and related user controls are listed here. You can decide whether you would like to allow your end users to use these services. For more information, see How admins can manage controller services in Office 365 ProPlus. If these optional services process personal data, Microsoft is a data controller for these services."*[152]

In this same guidance Microsoft also indirectly refers to its collaboration with the US based company UserVoice to collect user feedback: "*User feedback: If your users elect to provide feedback on Microsoft products and services, Microsoft is a data controller for such feedback to the extent it contains personal data. Microsoft fulfils any data subject requests for feedback collected by Microsoft (including feedback managed by Microsoft subprocessors) except in cases where Microsoft has instructed users not to include personal data during the feedback collection process. Exceptions: If Microsoft has instructed users not to include personal data during the feedback collection process, Microsoft relies on that instruction and will assume that no personal data has been provided. Users who have created a separate account with third-party feedback service providers need to fulfil their DSR directly with those providers."*[153]

5.4.3 Disclosure to law enforcement

In its new OST and DPA since January 2020 Microsoft has included a list of specific purposes of data processing 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 in May 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 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.

5.5 Joint controllers

According to three judgments of the European Court of Justice[154] parties can factually become joint controllers, even if the roles are unevenly distributed, and also if the

[152] Microsoft, Office 365 Data Subject Requests for the GDPR and CCPA,29 January 2020, URL: https://docs.microsoft.com/en-gb/microsoft-365/compliance/gdpr-dsr-office365
[153] Idem.
[154] 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.

party that is the customer does not have access to the personal data processed by the party that supplies a service.[155]

Because the use of Office for the Web is included in the Office 365 license, government organisations actually enable Microsoft to collect the telemetry data, and transfer personal data to third parties. The administrators can switch off the traffic to Giphy, but not the traffic to Optimizely. The administrators have no control at all over the telemetry events from Office for the Web: they cannot minimize the level and cannot inspect the data with a Data Viewer Tool or equivalent tool. As a result, the government organisations become joint controllers with Microsoft for these two types of processing.

If government organisations do not block the use of the mobile Office apps to the work environment for employees, they also enable Microsoft to process personal data about the use of the mobile Office apps for its own 17 purposes. In practice, therefore, the government organisations also become joint controller for these data processing operations with Microsoft.

Section 3.1 explains that Microsoft has created two privacy controls: to minimise the telemetry level and to disable all or only the Controller Connected Experiences. Unfortunately, these options do not yet function for all of the tested applications. As long as the government organisation are not in a position to determine (in this case: exclude) the purposes of the processing, in practice they also become joint controller for these data processing operations with Microsoft.

As explained in Section 4.2 above, Microsoft reserves the right as (joint) data controller to process the personal data for all seventeen purposes set out in its general privacy statement. As a result of being joint controllers, the government organisations can be held accountable for the processing of personal data relating to all kinds of data subjects for these purposes.

6. Interests in the data processing

This section outlines the different interests of Microsoft and the Dutch government organisations. The interests of the Dutch government organisations may align with the interests of its employees. 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 Dutch government organisations is analysed in part B of this DPIA.

6.1 Interests of the Dutch government organisations

The Dutch government organisations have security, efficiency and compliance reasons to switch to Office 365 and related services, such as SharePoint Online/OneDrive for Business and the Exchange Online servers.

The Office 365 cloud products offer the possibility to share information with each other instead of distributing it (as an attachment in the mail). Similarly, file sharing is easier and safer with OneDrive for Business. Many organisations still share files via network drives for document storage or via local SharePoint servers. In practice, employees share information via consumer versions of cloud products because existing solutions

[155] Umbrella-DPIA Office 365 ProPlus for SLM Microsoft Rijk, 7 November 2018, p. 48-50.

with network drives and SharePoint 2013 are not sufficient. Many people use, for example, G-Suite, Dropbox, WeTransfer and Google Docs to share files. This can result in a parallel network that the government organisations 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 Online and OneDrive for Business 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.

The government organisations have a strong general interest in providing reliable, always on, well integrated and location independent productivity tools to their employees. Well-functioning for the Dutch government also means that the software has to be accessible on different kinds of devices, and from different locations. The ability for employees to seamlessly work at home through for example collaboration tools like Teams. The use of Office for the Web and the mobile Office apps allows the government to cut back spending on work spaces in offices. Because Microsoft Office is also widely used in the consumer version, it is to be hoped that the software will also require less support from employees than competing software.
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. This information is necessary in order to be able to detect possible security incidents and to be able to end security or data breaches.

Last but not least, the Office 365 cloud products have the ability to explicitly and intrinsically secure information, by using encryption such as Customer Lockbox. Office 365 can automatically implement encryption policies and automatically label both existing and new documents and mails.

On the other hand, the Dutch government has a security and geopolitical interest in storing data in local data centres or, alternatively, in a limited number of data centres in the EU. The Ministry of Defence has a military state sovereignty interest to only store data in a sovereign cloud.

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 less effective.

Microsoft wants to be cloud first and mobile first since 2014.[156] 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*

[156] 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/.

one. It's evolved into a devices ecosystem rather than a single productivity device (…)."[157]

Microsoft has explained to SLM Microsoft 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.*"[158]

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. Microsoft provides Office 365 in various subscription forms, packaged with other online services. The vision of Microsoft is cloud-first, and pricing schemes strongly encourage the Dutch government to switch from on-premise deployments to cloud only services. Microsoft is effectively putting pressure on institutions to switch to the monthly model because it will soon end its support for older versions, such as Office 2010.

Microsoft has also spoken about 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 good enough, but we need to distinguish ourselves with advanced productivity scenarios.*"[159]

Nonetheless, as a result of the 2019 negotiations with SLM Microsoft Rijk, Microsoft - when it acts as a data processor- is prohibited from using personal data from government organisations in the Netherlands to show personalised recommendations for products or services of Microsoft the government organisations have not purchased or do not use.

Microsoft 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".[160] Microsoft earned more than 7 billion dollars in the period from June 2017 to June 2018 with the sale of targeted advertisements in its search engine Bing, on a turnover of more than 110 billion US dollars.[161] Microsoft writes about this in its 2018 annual report: "*Our Search business,*

[157] Idem.
[158] Microsoft Meeting report 30 August 2018, answer to Q46, quoted in the first public DPIA report on Office 2016 and Office 365 ProPlus.
[159] Idem, Meeting report 29 August 2018, answer to Q16.
[160] Idem, answer to. Q30.
[161] Microsoft Corporation Annual Form 10-K for the broken financial year 2017-2018 for the US financial regulator SEC, p. 94, URL: https://c.s-microsoft.com/en-us/CMSFiles/MSFT_FY18Q4_10K.docx?version=b04fa6cd-ed0e-a4ea-6f4f-

including Bing and Bing Ads, is designed to deliver relevant online advertising to a global audience […] Growth depends on our ability to attract new users, ***understand intent, and match intent with relevant content and advertiser offerings***."[162]

Microsoft does not offer a sovereign country cloud to countries, with the exception of the cloud for China, the German cloud (no new customers accepted[163]), and the separate cloud for the federal USA government. The costs to build a separate cloud for the Netherlands would be amount to, according to Microsoft, approximately 90 million US dollars. Microsoft has built its cloud to be able to process data anywhere where it operates (with the exception of China, USA FedGov, and Germany). This relates to the economies of scale. Therefore Microsoft only makes commitments about storage of Customer Data in specific data centres in the EU, not about other types of data.[164] If Microsoft would have to commit to more local or EU storage, this would involve high costs and be a barrier to innovation, according to Microsoft.[165]

6.3 Joint interests

The interests of Microsoft and the Dutch government align when it comes to the use of diagnostic data to protect the integrity, availability, and reliability of personal data in its 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, provided that the updates do not disrupt the service and that the technical administrators are able to disable or adjust the updates.[166] Similarly, the interests are aligned that Microsoft needs to deliver a well-functioning (bug free) product, for the Dutch government to prevent loss of labour capacity.

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

The GDPR contains special rules for the transfer of personal data to countries outside the European Economic Area (EEA), in articles 44 to 49. In principle, personal data may only be 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.

05c9f644b8a2_FY18Q4_10K.docx?version=b04fa6cd-ed0e-a4ea-6f4f-05c9f644b8a2. Microsoft explains that its business cloud services revenue for this period was $23.2 billion.

[162] Idem, p. 10.

[163] 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

[164] Meeting report 29 August 2018, answer to Q21.

[165] Meeting report 29 August 2018, answer to Q21.

[166] To the extent legally allowed without separate consent by the ePrivacy Directive and future ePrivacy Regulation. Roughly summarised, 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.

The European Commission can take a so-called adequacy decision. This means that the country in question has a level of protection comparable to that applied within the EEA. In addition, the EU and the USA have made separate agreements on the level of protection of personal data. Via the Privacy Shield (formerly: Safe Harbour), US companies can self-certify as to their standard of protection of personal data. In that case, data controllers in the EU may transfer personal data to such a company.
Personal data may also be transferred from the EU to a third country using Standard Contractual Clauses (SCC, also known as model clauses) drawn up by the European Commission on the basis of the (previous) Data Protection Directive. These clauses (hereinafter: SCC) contractually ensure a high level of protection. Microsoft uses a combination of two measures: Privacy Shield and the SCC.

The SCC apply to the transfer of personal data from online services such as Office for the Web and the Processor Connected Experiences (for which Microsoft is a processor). However, the transfer of diagnostic personal data from the Controller Connected Experiences and the mobile Office apps takes place on the basis of the EU-U.S. Privacy Shield. Microsoft has self-certified itself under this instrument.[167] Although both transfer instruments are legally valid, and have been approved by the European Commission, there are serious doubts about the future validity of these instruments for transfer to the US. Both instruments are the subject of proceedings before the European Court of Justice. The Court has been asked to decide whether these agreements offer sufficient protection against the risks of mass surveillance in the United States. These risks have been revealed by whistle blower Edward Snowden, also with regard to the interception of data in transit.[168]

In the OST[169], Microsoft guarantees that the subcategory of content data of the Core Online Services, which Microsoft defines as *Customer Data*, will only be stored in data centres in the EU. Microsoft does not offer the possibility to administrators to have the diagnostic data about the use of the different parts of the Office 365 license processed in the EU.

The diagnostic data (both the telemetry data and the system-generated log files) are directly transferred or generated on Microsoft servers in the USA. With regard to the Azure AD log files, Microsoft writes that these logs are initially stored in the data centre where the Azure AD service is running, i.e. in the case of Dutch government organisations in data centres in the Netherlands and Ireland. "*Log files are (..) originally created and stored in Azure storage in the data centre where the Azure AD*

[167] Microsoft is an active participant in the Privacy Shield Framework https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK&status=Active.
[168] In Case C 311/18, the AG Henrik Saugmandsgaard Øe of the European Court of Justice gave an advisory opinion on 19 December 2019 on the transfer from Facebook Ireland to Facebook Inc. in the US on the basis of the Standard Contractual Clauses. The AG observes that contractual agreements between parties are very different from the assessment of adequacy by the European Commission in the Privacy Shield. Controllers, or data protection authorities if the controllers themselves do not intervene, should themselves (order to) stop the transfer if there is a conflict between obligations under the Standard Clauses and the obligations in the country of destination, such as for example a legal obligation to comply with orders to provide personal data. However, if there is such a conflict, data controllers usually cannot have knowledge of such a conflict if the recipient is not allowed to inform the data controller about such orders. The AG does not formally give advice on the validity of the Privacy Shield, but nevertheless explains why he has doubts about the legal validity. There is another case pending before the ECJ concerning the Privacy Shield, case T-738/16. The application was lodged by the French NGO La Quadrature du Net on 9 December 2016. The hearing before the Court was to take place on 1 and 2 July 2019, but has been postponed until after the Schrems-2 judgment.
[169] OST March 2020.

service is running".[170] But subsequently, these log files are scrubbed and stored in Microsoft's long-term database in the U.S (see section 8.1 *Azure AD log files and usage data*).

Microsoft also writes that the Azure AD data processed with multi factor authentication are always processed exclusively in two data centres in the U.S., in Iowa and in California.[171] Microsoft writes: "*All two-factor authentication using phone calls or SMS originate from U.S. datacenters and are also routed by global providers.*"[172] This also applies to digital push messages. Microsoft writes: "*Push notifications using the Microsoft Authenticator app originate from U.S. datacenters. In addition, device vendor specific services may also come into play and these services maybe outside Europe*."[173]

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 unlawful 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. This differs, for example, for Outlook and for the SharePoint Online Customer Data. Content data from SharePoint and OneDrive for Business are stored in data centres in the Netherlands and Ireland.[174]

Microsoft may be ordered by U.S. courts to grant access for law enforcement to data stored in data centres in the EU. The U.S. CLOUD 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 European Data Protection Board and the 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 Article 6 (lawfulness of processing) and Article 49 (derogations for specific situations). In case of an order based on the US

[170] Microsoft, Data residency and customer data for Azure Multi-Factor Authentication, 16 December 2019, URL: https://docs.microsoft.com/nl-nl/azure/active-directory/authentication/concept-mfa-data-residency
[171] Microsoft, Identity data storage for European customers in Azure Active Directory, 4 March 2019, URL: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-data-storage-eu
[172] Idem.
[173] Ibid.
[174] Microsoft, Where is your data located, URL: https://products.office.com/nl-NL/where-is-your-data-located?ms.officeurl=datamaps&geo=Europe#Europe

CLOUD Act, the disclosure and transfer can only be valid if recognised by an international agreement between the EU and the USA.

The DPAs 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).*"[175]

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.*[176] Additionally, the data protection authorities refer to the ongoing negotiations 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.[177]

Access to Customer Data from the services that Microsoft considers to be Core Online Services is audited according to the strict standards of SOC-2. Access to Customer Data from 'other' services such as Office 365 ProPlus is audited for compliance with the ISO 270001 standard. There is no public documentation of any audits on diagnostic data collected through the Controller Connected Experiences and the mobile Office apps.

Sections 2.2 to 2.5 of this report describe the different types of diagnostic data that Microsoft collects through the mobile Office apps, the use of Office for the Web, the use of the Connected Cloud Services and the use of the Connected Experiences. All these data are either sent to Microsoft servers in the USA or generated on Microsoft servers in the USA.

Microsoft publishes a list of Office 365 network endpoints. Annex 1 to this report lists several third-party endpoints to which Microsoft transfers data.

The data can be analysed wherever Microsoft has computing capacity.[178] Microsoft does not want to commit to the storage of diagnostic data in the EU, as this would only be a cosmetic solution. The diagnostic data are analysed in the US and processed in a short-term database (30 days) and a long-term database (18 months). See section 10 of this report for a description of the retention periods.

[175] 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.
[176] Idem, cover letter.
[177] 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.
[178] Microsoft, URL https://docs.microsoft.com/en-gb/office365/enterprise/office-365-endpoints especially Worldwide endpoints, https://docs.microsoft.com/en-gb/office365/enterprise/urls-and-ip-address-ranges

8. Techniques and methods of the data processing

As explained in section 2 of this report, Microsoft collects personal data about the use of the mobile Office apps, Office for the Web and the connected cloud email and storage services in three ways. These are all diagnostic data according to the definition used in this report (see section 1.2). A fourth way Microsoft collects diagnostic data is described below: through the Azure AD usage and multi factor authentication log files.

Through the diagnostic data Microsoft also collects content data. On the one hand, in the system-generated server logs on its cloud servers, about the individual use of SharePoint Online, OneDrive for Business and Exchange Online. The technical research shows that Microsoft collects the same content (user-, path- and filename) data via some telemetry events from Office for the Web.

Microsoft also collects content data from the content of files, emails or chats when a user uses a Connected Experience, such as a spell checker.

8.1 Azure AD log files and usage data

In addition to the diagnostic data about the use of Office for the Web, about the mobile Office apps, and about the use of the Connected Cloud Services, Microsoft collects and processes two types of personal information about the use of the Azure Active Directory. The first category consists of log files that Microsoft collects and processes for its own purposes for auditing, research, usage analysis, correction of software errors (debugging), system health analysis and system-wide analysis with machine learning. Microsoft indicates that these files contain usernames. Microsoft writes that it removes personal data from the log files (scrubbing) before processing the data in the machine learning systems for general analysis.

In a whitepaper on the Azure AD data security considerations Microsoft writes: "*Log files are used for local debugging, usage analysis, and system health monitoring purposes, as well as for service-wide analysis. Prior to any system-wide analysis, log files are first scrubbed of personal data, which is tokenized. These logs are then copied over a secure SSL connection to Microsoft's reporting machine learning systems, which are contained in Microsoft owned data centers in the Continental United States.*"[179]

Besides the log files, Microsoft describes that it collects a category "Usage data" about Azure AD. Not only for clients, but also for itself, to analyse system use and improve the service. Microsoft states that it removes personal data before processing the data for this category.

Microsoft writes: "*Usage data is metadata generated by the Azure AD service that indicates how the service is being used. This metadata is used to generate administrator and user facing reports* ***and is also used by the Azure AD engineering team to evaluate system usage and identify opportunities to improve the service.*** *This data is generally written to log files, but in some cases, is collected directly by our service monitoring and reporting systems. personal data is stripped out of Microsoft's usage data prior to the data leaving the originating environment.*"[180]

[179] Microsoft Whitepaper, Azure Active Directory Data Security Considerations, Version: 2.01 Published: October 2019, URL: https://aka.ms/aaddatawhitepaper /
[180] Ibid.

The removal (erasure or deletion) of personal data after its collection is a processing of personal data. The GDPR applies to this processing. The fact that Microsoft deletes certain personal data from the log files makes no difference to the assessment that Microsoft processes personal data via these log files.

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 the Office 365 and the Connected Experiences. Microsoft has previously explained to SLM Microsoft Rijk hat prior to 2018 there were no central rules governing the collection of diagnostic data.[181] Since 2018 rules are in place, according to Microsoft. "*All **new** events proposed for diagnostic data collection from Office ProPlus Applications are reviewed by privacy trained and focused members of each engineering team, established standards for what may be collected are enforced, and documented sign-off prior to release provides accountability for decisions made. The data points are reviewed to ensure they meet the standards set for diagnostic data collection (i.e., that the data is necessary to keep the product secure, up to date, performing properly, and does not contain Customer Data). Currently 60 of these "privacy drivers" are distributed across Office engineering teams."*[182]

Microsoft has not published any information on rules regarding the collection of information by the Connected Experiences or the mobile Office apps. Microsoft stores the telemetry data from Office 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.[183] The engineer explains: "*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.[184]

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

a. *Bing, MSN, Hotmail, Client telemetry*
b. *Web crawl snapshots*
c. *Structured data feeds*
d. *Longtail of other data sets of interest"*[185]

Given the outgoing data traffic to UserVoice and Helpshift from the mobile Office apps, as described in section 2.2 of this report, Microsoft could receive profiles from these companies, and combine these profiles with the diagnostic data as 'data sets of interest'. As cited in Section 4.2 of this report, Microsoft, as a controller/supplier of consumer services, contractually allows itself to analyse data from various sources to

[181] Meeting report 28 August 2018, answer to Q1.
[182] Microsoft confidential response to the first public Office 365 ProPlus DPIA report, 24 September 2018, p. 10.
[183] 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)
[184] Ibid, slides 8 and 13.
[185] 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).

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 data, both on its own cloud servers and through the telemetry clients built into the mobile Office apps. 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.

As outlined in the investigation report of the Dutch DPA about Windows 10 telemetry data, certain rules from the current ePrivacy Directive may apply to the placing of information on, and retrieval of that information from, software installed on devices through an inbuilt telemetry client that is delivered via the Internet. Article 5(3) of the ePrivacy Directive has been transposed in Article 11.7a of the Dutch Telecommunications Act. Consent is required prior to the reading from or placing of information on the devices of end-users, unless one of the exceptions applies, such as necessity to deliver a requested service, or necessity for the technical transmission of information. The same consent requirement applies to the capturing of information about the use of the mobile Office apps on the iOS and Android mobile devices and sending information over the Internet.

The consequences of this provision are far-reaching, as it requires clear and complete information to be provided to the user prior to data processing. Part B of this DPIA discusses the (im-)possibility of obtaining valid end user consent for the processing of the diagnostic data from the mobile Office apps.

The current ePrivacy Directive (as transposed in the Netherlands in Chapter 11 of the Telecommunications Act) 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 current ePrivacy Directive do not apply to providers of software in the cloud (even though this always involves communication via a public electronic communications network), the future ePrivacy Regulation will make these rules applicable to Microsoft as a provider of e-mail and voice services.[186]

[186] See consideration 22 in the ePrivacy directive 2002/58/EG, revised in 2009 by the Citizens' Rights Directive 2009/136/EG: "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."

On 10 January 2017, the European Commission published a proposal for a new ePrivacy Regulation.[187] The proposed Article 8(1), *Protection of information stored in terminal equipment of end-users and related to or processed by or emitted by equipment*, extends the current consent requirement for cookies and similar techniques to the use of all processing and storage capabilities of terminal equipment.

The European Parliament adopted its position on 23 October 2017. It added a specific exception for updates and in relation to employees. The EP proposes to add two new exceptions to the consent requirement in Article 8(1), namely if it is necessary for security updates and for the performance of work by employees.

it is necessary to ensure security, confidentiality, integrity, availability and authenticity of the terminal equipment of the end-user, by means of updates, for the duration necessary for that purpose, provided that:

(i) this does not in any way change the functionality of the hardware or software or the privacy settings chosen by the user;
(ii) the user is informed in advance each time an update is being installed; and
(iii) the user has the possibility to postpone or turn off the automatic installation of these updates;

The EP also proposed:

in the context of employment relationships, it is strictly technically necessary for the execution of an employee's task, where:

(i) the employer provides and/or is the user of the terminal equipment;
(ii) the employee is the user of the terminal equipment; and
(iii) it is not further used for monitoring the employee.

The Council of Ministers has been debating the e-Privacy Regulation for two and a half years, since October 2017. The most recent complete text dates from 6 March 2020.[188]

In a first complete concept, published on 19 October 2018, the Council proposed to follow Parliament's line with regard to employees and security updates. The representatives of the Member States also wanted to allow employers to base processing operations on employees' consent, without any reflection on the conflict with the legal presumption in article 7(4) of the GDPR and recital 43 that consent cannot be given freely if there is a clear power imbalance between the data subject and the controller.

The Council's proposal for Article 8 of the ePrivacy Regulation has significantly been amended since February 2020, by introducing a general legitimate interest ground. The Council proposes to rename Article 8: *Protection of end-users' terminal equipment information.*

(Art 8 (1) The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its

[187] 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

[188] Council of the European Union, Interinstitutional file 2017/0003 (COD), Brussels 17 October 2019, 13080/19 URL: https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=consil:ST_14447_2019_INIT .For an overview of the earlier proposed versions of the regulation by the council, see: https://eur-lex.europa.eu/procedure/EN/2017_3#2019-11-08_DIS_byCONSIL .

software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:
(…)
(c) it is necessary for providing a service requested by the end-user;
~~(da): it is necessary to maintain or restore the security of information society services, prevent fraud or detect technical faults for the duration necessary for that purpose;~~
~~or~~
~~(e) it is necessary for a software update provided that:~~
~~(i) such update is necessary for security reasons and does not in any way change the privacy settings chosen by the end-user,~~
~~(ii) the end-user is informed in advance each time an update is being installed, and~~
~~(iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates; or~~
(g) it is necessary for the purpose of the legitimate interests pursued by a service provider to use processing and storage capabilities of terminal equipment or to collect information from an end-user's terminal equipment, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user. The end-user's interests shall be deemed to override the interests of the service provider where the end-user is a child or where the service provider processes, stores or collects the information to determine the nature and characteristics of the end-user or to build an individual profile of the end-user or the processing, storage or collection of the information by the service provider contains special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679.[189]

The Council explains in the new recital 21b:

A legitimate interest could be relied upon where the end-user could reasonably expect such storage, processing or collection of information in or from her or his terminal equipment in the context of an existing customer relationship with the service provider.
For instance, maintaining or restoring the security of information society services or of the end-user's terminal equipment, or preventing fraud or detecting technical faults might constitute a legitimate interest of the service provider.
Similarly, using the processing storage capabilities of terminal equipment is to fix security vulnerabilities and other security bugs, provided that such updates do not in any way change the functionality of the hardware or software or the privacy settings chosen by the end-user and the end-user has the possibility to postpone or turn off the automatic installation of such updates. Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not be considered as a legitimate interest.

The Council proposes to add an exception for security purposes to Article 6, with rules on the processing of electronic communications data (both content and traffic data)

Article 6
1. Providers of electronic communications networks and services shall be permitted to process electronic communications data only if:
(…)
(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors and/or security risks and/or attacks in the transmission of electronic communications, ~~for the duration necessary for that purpose;~~

[189] Idem.

(c) it is necessary to detect or prevent security risks and/or attacks on end-users' terminal equipment, ~~for the duration necessary for that purpose.~~[190]

With regard to the basis for employees, the Council proposes in its latest version of 6 March 2020, in the renumbered recital 16c to strike its previous insistence of consent from employees as a legal ground.

Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal person having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service in accordance with Regulation 2016/679.

With regards to the use of the processing and storage capabilities of terminal equipment, the Council has deleted explanations when consent would be required from recital 21:[191]

Use of the processing and storage capabilities of terminal equipment or to access to information stored in terminal equipment without the consent of the end-user should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of providing a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages, authentication session cookies used to verify the identity of end-users engaged in online transactions or cookies used to remember items selected by the end-user and placed in shopping basket. In the area of IoT services which rely on/deploy connected devices (such as connected thermostats, connected medical devices, smart meters or automated and connected vehicles), the use of the processing and storage capacities of those devices and access to information stored therein should not require consent to the extent that such use or access is necessary for the provision of the service requested by the end-user. For example, storing of information in or accessing information from a smart meter might be considered as necessary for the provision of a requested energy supply service to the extent the information stored and accessed is necessary for the stability and security of the energy network or for the billing of the end-users' energy consumption (…)
~~To the extent that use is made of processing and storage capabilities of terminal equipment and information from end-users' terminal equipment is collected for other purposes than for what is necessary for the purpose of carrying out the transmission of an electronic communication over an electronic communications network or for the provision of the service requested, consent should be required. In such a scenario, consent should normally be given by the end-user who requests the service from the provider of the service.~~

In sum, it appears that the ePrivacy Regulation continues to contain a consent requirement for the collection of information from devices from users where this is not necessary to provide a service. In its last version the Council proposes to introduce the legitimate interest ground. This is diametrically opposed to the position of

[190] Idem. This article was initially article 6 (1). The limitation of the duration of processing is included in a separate second section: "*Electoronic [sic] communications data shall only be permitted to be processed for the duration necessary for the specified purpose or purposes according to Articles 6 to 6c and if the specified purpose or purposes cannot be fulfilled by processing information that is made anonymous.*"
[191] Idem.

European Parliament and Commission. It therefore seems likely that the current ePrivacy Directive, which does not contain such a balancing of interests possibility, will continue to apply in the next few years.[192]

10. Retention periods

In the Data Protection Addendum belonging tot the public OST of March 2020 Microsoft has included one section on retention periods. This shows that Microsoft retains Customer Data for another 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 Microsoft Rijk, it has been agreed that Microsoft will not store personal data for longer than 18 months after the initial collection.

Since May 2019, Microsoft has published a little more information about the various retention periods for Personal Data in Office 365.[193]

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

Table 3: Microsoft overview of data types and retention periods

1	Customer Content	30 days after the administrator has actively deleted the data, or passively, 180 days after the termination of the subscription

[192] It is not clear when the new ePrivacy Regulation (2017/0003/COD) will enter into force. Progress can be tracked via: https://eur-lex.europa.eu/procedure/EN/2017_3 The Ministers of the Member States have not yet reached agreement in the Council (in March 2020) on their negotiating position on the ePrivacy Regulation. Thereafter, the trialogue should start negotiations with the (new) European Commission and the (new) European Parliament. Subsequently, a transitional period of 1 or 2 years will apply. In any case, the scope of the scope of the Telecommunications Directives and the ePrivacy rules will be extended via the Electronic Communications Code (2016/0288(COD), final vote by the European Parliament on 14 November 2018) after a transitional period of 2 years, at the end of 2020, from the current handful of providers of telephony and Internet services to all web-based equivalent providers.
[193] Microsoft, Data Retention, Deletion, and Destruction in Office 365, 6 May, URL: https://docs.microsoft.com/en-gb/office365/securitycompliance/office-365-data-retention-deletion-and-destruction-overview

2	Content conversations in Teams	Six months[194]
3	Directly identifiable personal data, as user and/or screenname, IP-address	180 days, both at actively and passively deletion
4	Other pseudonymous personal data	30 to 180 days

The table describes how long Microsoft retains data after a customer actively deletes the data, or after a customer terminates the subscription (passive deletion). But this table is far from complete. Microsoft only describes unique identifiers in this table, but not the usage data. Microsoft fails to explain that it records and stores the individual actions of users in combination with the named identifiers.

Discussions between SLM Microsoft 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. This means that if an employee joined an organisation in 2005, for example, Microsoft would have been able to collect and store historical diagnostic data about that person's behaviour for fifteen years, if no other removal rules applied.

Microsoft mentions a shorter retention period for the system-generated log file category in a document called *Guidance for data controllers to conduct a Data Protection Impact Assessment*. Microsoft explains that these files are stored for at least six months, or as much longer as necessary for the security of the services: "*This data is retained for a default period of up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.*"[195]

The table does not explain the retention period of the audit log files and does not address Microsoft's need for an 18-month retention period for the telemetry data.

Microsoft has provided SLM Microsoft Rijk with a statement about retention periods. In the document Microsoft explains it has two different retention periods for the diagnostic data from Office 365.

"The diagnostic data is stored in two Microsoft systems, one providing a short term storage facility (designated herein as "K") and one providing a longer term storage facility (designated herein as "C"). The stored data in these systems is subject to access controls to ensure that access and use of the data by Microsoft personnel and subprocessors is for permitted purposes.

System "K" stores the diagnostic data (including personal data contained therein) for 30 calendar days from the time of receipt at Microsoft as described above. These data are used by engineers working on immediately relevant diagnostic scenarios such as the impact of security threats and their remediation, or the efficacy of recently

[194] 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."

[195] Data Protection Impact Assessments: Guidance for controllers using Microsoft Office 365. Available at https://docs.microsoft.com/en-gb/microsoft-365/compliance/gdpr-dpia-Office 365 (URL last visited and recorded on 8 July 2019).

implemented changes in the Office 365 ProPlus software at ameliorating software and service problems. The data stored in short term storage systems are also used in scenarios where Microsoft is proactive in assisting customers encountering problems in their environment.

System "C" stores the diagnostic data (including personal data contained therein) for 18 months from the time of receipt at Microsoft as described above. These data are used in scenarios where evaluation of the efficacy of fixes, changes, or updates in software and services will manifest in the longer term, including year over year. This condition arises because customers can choose to deploy Microsoft updates at different cadences, some of which may be up to a year after Microsoft has released a fix, change, or update to the software. Therefore, Microsoft needs to retain the diagnostic data for longer than one year in order to be able to achieve this diagnostic purpose across a complete deployment cycle, but does not need to retain the diagnostic data beyond 18 months to achieve that goal."

Microsoft explains that the individual government organisations cannot change the retention periods of the diagnostic data. Microsoft writes: "*customer-specific diagnostic data retention practices are not supported. The Online Services are a hyperscale public cloud delivered with standardized service capabilities made available to all customers. Beyond configurations available to the customer in the services, there is no possibility to vary operations at a per-customer level. Accordingly, we cannot support a customer-specific commitment related to storage duration for diagnostic data.*"[196]

Microsoft does not offer a possibility to delete outdated diagnostic data from Office 365 ProPlus, Office for the Web or the mobile Office apps 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.[197]

Retention periods for audit logs Connected Cloud Services

Microsoft describes a 90-day retention period for the audit logs, which contain detailed information about the individual actions a user performs in SharePoint Online, OneDrive for Business and Exchange Online, together with content data such as email subject lines and file names. Microsoft writes: "*Note that auditing records are retained for 90 days. Therefore, you won't be able to search for user activities that occurred more than 90 days ago.*"[198]

Microsoft describes on a separate page about SharePoint Online Data Deletion that it saves the content data (Customer Data) from SharePoint for 93 days after the file is deleted in its original location.[199] In Exchange Online, the default retention period for the deleted content data is 14 days, but an administrator can extend this period to 30 days.[200]

---

[196] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q8 (preamble).
[197] Ibid, answer Q8b.
[198] Microsoft, Office 365 Data Subject Requests for the GDPR, Use the Office 365 audit log search tool in DSR investigations, 6 April 2019, URL: https://docs.microsoft.com/nl-nl/microsoft-365/compliance/gdpr-dsr-office365?toc=/microsoft-365/enterprise/toc.json
[199] Microsoft, SharePoint Online Data Deletion in Office 365, 1 April 2019, URL: https://docs.microsoft.com/en-gb/office365/securitycompliance/office-365-sharepoint-online-data-deletion "*In SharePoint Online, items are retained for 93 days from the time you delete them from their original location. They stay in the site Recycle Bin the entire time, unless someone deletes them from there or empties that Recycle Bin.*"
[200] Microsoft, Exchange Online Data Deletion in Office 365, 29 maar 2019, URL: https://docs.microsoft.com/en-gb/office365/securitycompliance/office-365-exchange-online-

Retention period central Cosmos database

In the table above, Microsoft only describes the retention periods for active and passive deletion of the content Customer Data, not the retention periods it determines itself in central database systems such as Cosmos. As quoted above, Microsoft stores most of the telemetry data from Office 365 for 30 days, but also stores certain data for a long period of time in Cosmos, up to 18 months.

A Microsoft document with the checkpoints for compliance with the American NIST cybersecurity standard shows that Microsoft also stores the system-generated log files from Office for the Web and the Connected Cloud Services in the central Cosmos database. The unique user identifiers from the audit logs are replaced by hashes, but the service teams can undo this form of pseudonymisation. The NIST audit document describes:

"*The tools used by Microsoft to collect and process Office 365 audit records do not permanently or irreversibly alter the original audit record content or time ordering. Microsoft scrubs logs of customer information before sending logs to Cosmos.* ***Cosmos is the central audit record repository for all service teams, and audit logs are uploaded to Cosmos from all servers in the Office 365 environment****. Specifically, scrubbing takes fields containing customer data, hashes that data, and replaces the field with the hash value. The rewritten log is sent to Cosmos, while each service team stores a mapping of hash keys to hashes within the Office 365 accreditation boundary. Cosmos can then correlate, alert, and report on these anonymized hashes.* ***If an alert or report requires investigation, the logs are imported back inside the boundary. The service team can then repopulate the logs to their original state using the hash key to hashes mapping.*** *Use of Cosmos is protected via Office 365 Interconnection Service Agreements with Cosmos, and the controls that Office 365 inherits directly from Cosmos were directly assessed by the third-party assessment organisation."*[201]

The NIST document explains that the only change Microsoft makes to the audit logs before transferring them to its Cosmos data warehouse, is to replace directly identifiable personal data with hash values. "*It was also noted that no data leaving the Office 365 boundary (Cosmos is located outside the boundary) can leave in clear text.* ***Thus, the only modification made to audit records being sent to Cosmos is part of the scrubbing process which includes replacing all personally-identifiable information (PII) with a hash value. (…) It was determined that once the PII is encrypted, the PII can be decrypted only by a user with the proper decryption key****."*[202]

Because this long retention period in Cosmos also applies to the telemetry events that Microsoft collects from Windows 10, Office for the Web and the system generated log

---

data-deletion "*When a user deletes a mailbox item (such as an email message, a contact, a calendar appointment, or a task), the item is moved to the Recoverable Items folder, and into a subfolder named Deletions. This is referred to as a soft deletion. How long deleted items are kept in the Deletions folder depends on the deleted item retention period that is set for the mailbox. An Exchange Online mailbox keeps deleted items for 14 days by default, but Exchange Online administrators can change this setting to increase the period up to a maximum of 30 days."*

[201] Microsoft Office 365 - Audited Controls NIST 800_53A Rev 4, published 11 April 2017 via the Security and Compliance Center, URL: https://protection.office.com/DownloadFile/ServiceAssurance/Document/othertrust/Office%20365%20Audited%20Controls%20NIST%20800_53A%20Rev%204/xlsx URL announcement with explanation: https://techcommunity.microsoft.com/t5/Office-365-Blog/Released-Office-365-Audited-Controls-for-NIST-800-53/ba-p/61479

[202] Idem.

files about the use of the cloud services, it is plausible that this also applies to the telemetry events from the mobile Office apps and from Office for the Web.

Back-ups

Microsoft has explained that it does not make backups the way people usually understand back-ups, as passive copies, possibly even on tape. Microsoft does *real-time* active-active replication, with a small delay in replication. Within a period of time, the other copy would get the same delete instructions.[203] This explains the difference between the initial retention period, and some period afterwards in which snippets of data may still be available in replications of the data.

Microsoft explains: "*Once the maximum retention period for any data has elapsed, the data is rendered commercially unrecoverable.*"[204] In its overview of results of audits by independent third-party auditors for compliance with NIST 800-53A (Rev. 4)[205] Microsoft explains*:*

"*Physical backups are not used in several services. Data is replicated using either Azure's built-in data replication, built-in service data replication, or complete redundant services. Other servers are stateless; server recovery consists of redeployment from standard images and scripts as described in the CM family of controls.*

Email databases and artifacts (mail trace information, MX records, spam definitions, etc.) are replicated between datacenters.

Standard images and scripts are used to recover lost servers, and replicated data is used to restore customer user-level data."[206]

Microsoft also explains: "*The SharePoint Online service team conducts weekly full backups and daily differential backups and backs up the transaction logs every five minutes. These point in time backups are retained for 15 days. Backups are replicated across multiple instances and sites.*"[207]

Microsoft explains that the back-up data are encrypted. "*All data that is backed up is encrypted prior to writing to disk, which protects both the confidentiality and integrity of the backed up data.*

Online backup data is stored within the accreditation boundary and protected via the same methods as production data. Data that is physically backed up is encrypted prior to writing to tape or disk, which protects both the confidentiality and integrity of the backed up data."[208]

[203] Meeting report 30 August 2018, answer to Q33.
[204] Microsoft, Data Retention, Deletion, and Destruction in Office 365, 6 May 2019.
[205] NIST is the National Institute of Standards and Technology. The controls date from 2014 and are for assessing security and privacy controls in federal information systems and organisations. URL: http://dx.doi.org/10.6028/NIST.SP.800-53Ar4
[206] Microsoft NIST 800-53A (Rev. 4), 8 May 2019, Control ID: CP-09(a) details in CP-0146, 'Information backup'. Accessible (with Microsoft account log-in) via the Microsoft Servicetrust dashboard, audited controls for Office 365.
[207] Idem, CP-09a, implementation details CP-0145
[208] Idem, CP-09d, implementation details CP-0148.

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 Office for the Web, Connected Cloud Services and Processor Connected Experiences

Thanks to the improved privacy terms that SLM Microsoft Rijk has 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 most of the diagnostic data processing (Office for the Web, the Processor Connected Experiences and the Connected Cloud Services). 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 Office for the Web, the Connected Cloud Services and the Processor Connected Experiences, government organisations 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.

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 employees are provided with the Office products to be able to carry out the tasks included in their job description. As described in section 6.1 of this report, the Dutch government has an interest in promoting teleworking. To this end, employees should be able to access work documents from different devices and different locations.

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, the organisation can successfully invoke this legal ground. This ground only applies to the extent the organisation requires employees to use the Office software to do their work. 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).

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.* Because the online Office services and mobile Office apps can also be used to communicate with other data subjects, government organisations can 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 may process a limited set of innocent diagnostic 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. This report recommends that government organisations perform a DPIA before they decide to use analytic services such as the Office 365 Reports in the Admin Center, MyAnalytics, Delve and Workplace Analytics. Such a DPIA should take the risks into account that the use of these analytics may have a strong chilling effect on employees, given the inevitability of spending many working hours with the productivity software of Microsoft (Office, Windows and other services and applications).

11.2 Telemetry data and traffic to third parties from Office for the Web

It follows from the technical research that Microsoft does not always factually behave like a processor in Office for the Web. Microsoft forwards personal data to two external companies in Teams and OneDrive in Office for the Web. These companies (Giphy and Optimizely) are independent data controllers and can process the data for their own marketing purposes. These processing operations do not fall within the three authorised purposes. As explained in section 5.4 of this report, this makes the government organisations joint controllers with Microsoft for the use of these services. The administrators can centrally block the traffic to Giphy, but not to Optimizely.

With regard to the telemetry messages from Office for the Web, it is not clear to what extent Microsoft acts as a processor or as a controller. In its response to the technical findings, Microsoft has stated that it "*uses internal software logic to maintain that when data is processed from Office 365 work or school accounts, any sub-processing of personal data and content is limited to the published list of subprocessors*." This explanation leaves a great deal of room for interpretation. It cannot be ruled out that Microsoft considers itself to be the data controller for the telemetry data from Office for the Web, because this data flow is separate from the data that logged in users themselves share and receive via the applications. Therefore, the government organisations should also be considered joint controllers with Microsoft for the telemetry data from Office for the Web.

As joint controllers for the processing of the telemetry data from Office for the Web and for the external data traffic to Optimizely, nor Microsoft nor the government organisations have a legal basis for the processing under the current circumstances.

Consent

Article 6 (1) (a) GDPR reads: "the data subject has given consent to the processing of his or her personal data for one or more specific purposes"

For employers it is almost impossible to obtain valid, freely given consent from employees, given the clear imbalance in the labour relationship. In this case, the data subjects (employees) have no choice with regard to the processing of their personal data by third parties when logging on to the OneDrive webpage, or about the collection of telemetry data by Microsoft about their use of Office for the Web. They cannot freely refuse to give their consent. In addition, the processing is untransparent and it is not clear for what purposes the two companies, or Microsoft itself, process the data. As joint controllers, Microsoft and the government organisations cannot rely on consent, even though such consent is required based on the Dutch Telecommunications Act when these data are processed for marketing and analytical purposes.

Contract

Microsoft and the government organisations cannot rely on the necessity to perform a (labour) contract. As explained in the previous public DPIA, Microsoft does not have an individual separate contract with the employees, and the processing of these data by Microsoft and by third parties is not necessary for the performance of the labour contract.

Legitimate or public interest

Unlike Office 365 ProPlus and the mobile Office apps, the administrators do not have the possibility to set the telemetry level to the lowest level 'Neither' for Office for the Web. They cannot inspect the content of the telemetry and Microsoft does not publish any information about the contents or its necessity to collect these data. The technical research shows that Microsoft collects content data such as username, file name, and pathname through this telemetry. In the absence of documented necessity for the

telemetry data processing via Office for the Web, the lack of a data minimisation option, the observed traffic to third parties and the sensitive nature of the data, Microsoft and the government organisations are also unable to successfully invoke the basis of necessity for the performance of a task carried out in the public interest or necessity to protect their legitimate interests. The other two legal grounds of the GDPR do not apply.[209]

11.3 Mobile Office apps and Controller Connected Experiences

As analysed in section 5.3, Microsoft considers itself to be an independent data controller for the mobile Office apps and the Controller Connected Experiences.

Consent

To the extent that Microsoft would want to rely on consent from the end-users to collect and send the telemetry data from the mobile Office apps to its own servers in the USA, Microsoft shows incomprehensible text in the app store and a hyperlink to the Privacy Statement. This should 'inform' users that Microsoft acts as a data controller, even if they download the apps as part of a government Office 365 license. This information obviously does not meet the thresholds of 'specific' and 'informed' consent.

Microsoft equally fails to obtain valid consent for the diagnostic data processing through the Controller Connected Experiences. Microsoft does not meet the requirements of specific and informed consent, because of the lack of explanation that this agreement applies to all Controller Connected Experiences, in all applications, and that this involves sensitive data processing, such as the scanning of Word documents to integrate resumes with LinkedIn.

In practice, the government organisations become joint controllers with Microsoft if they do not centrally block access from the mobile Office apps to the Office work environment and the Controller Connected Experiences. Microsoft contractually permits itself to process the diagnostic data for 17 purposes as described in its Privacy Statement. Consent is not an option for government organisations, given the power imbalance between employers and employees.

Contract, public and legitimate interest

As joint controllers with Microsoft, as described in section 11.1 the government organisations can only use the legal grounds of necessity for the performance of the agreement, necessity for the performance of a task carried out in the public interest or necessity for the legitimate interests for the three authorised purposes in the privacy amendment with the Dutch government.

Microsoft nor the government organisations have a legal ground for the processing of data from the mobile Office apps and the Controller Connected Experiences for any other purpose (such as transferring personal data to third parties for analytical and marketing purposes). These purposes are therefore lumped together in the table below.

Independently of this, as specified in the contract with SLM Microsoft Rijk, Microsoft sometimes has to act as an independent data controller, for example when it comes to the processing of customer data for annual financial statements and the sending of invoices. These purposes of processing fall outside the scope of this DPIA.

[209] When using the browser versions of the Office software, there is no vital life-saving necessity, no necessity for the performance of a public task or a specific legal obligation.

Table 4: Overview of the different legal grounds

Purpose	Legal ground	Government organisations as data controllers	Joint controllers	Microsoft as data controller
Type of data processing		*Contents and cloud logs Office for the Web, logs Connected Cloud Services, Processor Connected Exp, logs Azure AD*	*Telemetry Office for the Web, Telemetry mobile Office apps, traffic to 3d parties & Controller Connected Exp.*	*Same types of processing as joint controllers*
Providing the service, incl. troubleshooting and bug fixing	Consent	X	X	X
	Contract	√	X	X
	Legitimate & Public interest	√	X	X
Providing updates	Consent	X	X	X
	Contract	√	X	X
	Legitimate & Public interest	√	X	X
Security	Consent	X	X	X
	Contract	√	X	X
	Legitimate & Public interest	√	X	X
17 different purposes mobile Office apps and the Controller Connected Exp., including transfer of personal data to third parties	Consent	X	X	X
	Contract	X	X	X
	Legitimate & Public interest	X	X	X

In sum, nor Microsoft nor the Dutch government organisations have a legal ground for four of the processing operations that take place as a result of the use of Office for the Web and the mobile Office apps.

The Dutch government organisations can only obtain a legal ground for some of this data processing, but only if Microsoft acts as a data processor. It goes without saying that Microsoft should not send personal data to third parties, unless they are contractually bound to process the data as Microsoft's subprocessors, and thus limited to the processing for the three authorised purposes.

12. Special categories of data

As explained in section 2.10.1 of this DPIA, it is up to the individual government organisations to determine if they process special categories of 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.

Government organisations must determine if the specific data protection risks associated with the storing of these data on Microsoft's cloud computers (SharePoint Online or OneDrive for Business) require additional protection measures, such as encryption.

The data protection risks for data subjects are not limited to the processing of special categories of data. Similar risks may apply to other categories of personal data of a sensitive nature, classified or secret data. The EDPS explains in its guidelines on the use of cloud computing services by European institutions that special categories of data should be interpreted broadly when interpreting the risks for data subjects. The EDPS writes: "*Nevertheless, this is not the only factor determining the level of risk. Personal data that do not fall under the mentioned categories might lead to high levels of risk for the rights and freedoms of natural persons under certain circumstances, in particular when the processing operation includes the scoring or evaluation of individuals with an impact on their life such as in a work or financial context, automated decision making with legal effect, or systematic monitoring, e.g. through CCTV.*"[210] The EDPS also refers to the criteria provided by the Article 29 Working Party when a Data Protection Impact Assessment (DPIA) is required.[211]

Government organisations must consider the risk that special categories of data (or otherwise very sensitive data) could end up in file and path names stored in system generated log files from access to SharePoint Online and OneDrive for Business. Microsoft would process these data in its role as processor, but Microsoft also processes usernames, file and pathnames as part of the Office for the Web telemetry, and could very well consider itself data controller for this data processing. Government organisations should therefore take account of the general prohibition on the processing of special categories of data from articles 9 and 10 of the GDPR if they are joint controllers with Microsoft. There is no exception for the processing of these personal data by Microsoft for its own 17 purposes. The only general useful exception in Article 9 GDPR is if the data subject has given explicit consent. However, valid consent is not an option as explained in sections 11.2. and 11.3 of this DPIA. Article 10 of the GDPR completely prohibits the processing of personal data relating to criminal convictions and offences, if not under the control of official authority or when authorised by Union or member law.

12.1 Transfer of special, sensitive, secret and confidential data to the USA

Even though Microsoft guarantees that the Customer Data (the content data) are stored in data centers in Europe, these guarantees do not apply to the diagnostic data.

With regard to both types of personal data, there are risks related to unlawful further processing of personal data (i) through interception or orders from USA law enforcement authorities, security agencies and secret services, (ii) through rogue administrators at Microsoft and at subprocessors, and (iii) through hostile state

[210] EDPS, Guidelines on the use of cloud computing services by the European institutions and bodies, 10 March 2018, URL: https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf

[211] Article 29 Working Party (now: EDPB), WP 248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, URL: http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236 .

actors. The likelihood and impact of these risks are assessed in paragraph 16.2.9 of this report.

To mitigate some of these risks, government organisations can create policy rules to prevent that some very confidential data are processed by cloud services. They could also draft a policy to prohibit the use of directly identifying personal data in file and path names. Last but not least, they can consider extra protection possibilities such as encryption of data in SharePoint Online and OneDrive for Business.

Microsoft offers two relevant encryption services: 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.
- 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.

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 purposes for further processing of the personal data. A data processor, such as Microsoft claims to be for Office for the Web cannot decide itself what purposes it finds compatible.

Purpose limitation is the most difficult principle to comply with in *big data* processing. because it is precisely invented to gain new insights by combining data in a different way. The data processing is dynamic, as explained in section 8.2 of this report. At Microsoft there are 20 to 30 engineering teams working with Office telemetry data alone (and it is unknown how many other teams are working with other diagnostic data). They may all ask different questions, and add new telemetry events to answer new questions. Until 2018 there was no central rule in Microsoft against which an auditor could test if the existing or newly added events were legitimately added. Since the spring of 2019, Microsoft has made global improvements to the information about, and privacy controls for, the telemetry in Office 365 ProPlus. However, these privacy controls have not yet been implemented, or only partially implemented, for the mobile Office apps and Office for the Web. Microsoft does not publish any information about the telemetry from Office for the Web and the mobile Office apps.

Based on the privacy amendment with the Dutch government Microsoft is limited to process the diagnostic personal data collected from and about the use of Office for

the Web, the Connected Cloud Services and the Processor Connected Experiences for three authorised purposes, and only where proportional. Nevertheless, the technical research shows that some personal data are transferred via Office for the Web to two third parties, who may use the data for their own marketing purposes. As explained in section 5.4, Microsoft therefore acts as (joint) data controller. As explained in section 11.2, Microsoft and the Dutch government organisations that deploy Office 365, have no legal ground as joint controllers for this transfer of personal data to third parties. With regard to the telemetry events from Office for the Web, it also is insufficiently clear whether Microsoft acts as processor, and if so, whether the processing is limited to the agreed three purposes.

With regard to the processing for which Microsoft is the controller, the mobile Office apps and the remaining Controller Connected Experiences, Microsoft does not specify for what specific purposes Microsoft processes which data. As described in Section 4.2, Microsoft mentions seventeen purposes for data processing in its general privacy statement. Microsoft does not specify which types of personal data it processes for which purposes, and some purposes are so general (such as, for example, Research) that the description offers no insight what processing Microsoft does and does not allow itself to do under this purpose. With the mobile Office apps, Microsoft as a controller aims to fulfil an (alleged) interest of certain users in personalised advertising and targeted offers for Microsoft products and services (see Section 6 of this report, on the different interests in the data processing). In addition, the technical research shows that Microsoft sends traffic from the mobile Office apps to six external companies, four of which are not subprocessors. As explained in section 2.2, Microsoft sends personal data via the mobile Office apps on iOS to the German company Adjust (via the OneDrive and Outlook apps) and to four American companies. This is done from the Word app to Cloudflare, from the Outlook app to Helpshift and UserVoice and from the Teams app to Giphy.

As the data controller, Microsoft does not publish any information about the parties with which it cooperates in the provision of its consumer services. In its general privacy statement (which applies to the mobile Office apps), Microsoft explains that it may share personal information with third parties such as affiliates and vendors, but that these companies must comply with Microsoft's security and privacy requirements. The fact that Microsoft requires such third parties to comply with Microsoft's rules however does not mean that Microsoft has a subprocessor agreement with these parties as referred to in article 28 of the GDPR.

Section 2.2. of this report explains that Adjust, Cloudflare, Giphy, Helpshift and UserVoice have their own processing purposes, which do not fit within the three authorised purposes for which Microsoft, as processor, may process the personal data from Dutch government organisations. Even if Microsoft has a contract with UserVoice as a subprocessor, UserVoice expressly reserves the right to use the personal data collected for its own purposes. UserVoice even explicitly acknowledges that it thus acts as the data controller: "*We also use our own product to collect, store, and retrieve data to analyze our own product. In this capacity, we are both a data controller and data processor, since the data processing is happening for our own purposes.*"[212]

In its response of 6 March 2020 to the technical findings in this report, Microsoft stressed that it is an independent data controller for the data processing of the mobile Office apps. Furthermore, Microsoft has indicated that the traffic to third parties does

[212] UserVoice, GDPR Compliance, version 1.3, 6 April 2018, URL: https://www.UserVoice.com/gdpr-compliance/ .

not necessarily involve processing of content or personal data by a third party. If so, Microsoft ensures that traffic from signed-in work and school accounts only goes to the published list of subprocessors. Because the technical research has actually established that traffic does go to third-party companies when a user is logged in with a school or work account, and that this traffic at least always includes the user's IP address, this statement by Microsoft is incorrect. Microsoft's statement is also contradictory when it comes to traffic from the apps, because Microsoft simultaneously appeals to the voluntariness of, for example, the use of the two helpdesk functionalities in the Office apps. The degree of voluntariness can be disputed, because users are not warned, nor asked to consent, if they use these helpdesk functions, that their data will be shared with a third party in the USA.

In view of the lack of purpose limitation for the services for which Microsoft acts as (joint) controller, the government organisations can not trust that Microsoft will only process the telemetry data from Office for the Web and the mobile Office apps for legitimate 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.[213]

[213] 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*

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.

There is no public, centrally accessible source of information from Microsoft about the telemetry data it collects through Office for the Web and the mobile Office apps. Administrators and users can only view the telemetry messages from three Office apps in decoded form (Word, PowerPoint, and Excel), not from the other Office apps, and not at all from Office for the Web.

Microsoft also does not publish any information about the diagnostic data it collects through its own system-generated log files about use of its cloud storage, authentication and email services (SharePoint Online, OneDrive for Business, Azure AD and Exchange Online). Although administrators can request access to these data via the audit logs and via the automated access tool (see the results in section 2.5), the processing is insufficiently transparent. Due to Microsoft's lack of documentation, the results from the access requests cannot be compared with documentation stating why and for what purposes Microsoft collects these data.

There is a similar lack of transparency about the diagnostic data that Microsoft collects via the Processor and Controller Connected Experiences. As explained in section 2.8, Microsoft only provides five examples of messages that are stored on the individual's device and sent to Microsoft. These messages belong to a category of telemetry messages that administrators cannot disable at all, the so-called Required Service Data. Microsoft does not provide an overview of the diagnostic data generated in the system log files of the Microsoft servers offering the Connected Experiences. The audit log files and automated access requests do not contain any information either about the diagnostic data collected through the Connected Services. Although Microsoft writes that it hopes to make further privacy improvements in the coming months, it is not clear whether this will also lead to more access to, and public documentation about, the various Connected Experiences.

The lack of transparency makes the data processing inherently unfair. The lack of transparency also makes it impossible to assess the proportionality of the processing.

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 AVG). 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.

With respect to the diagnostic data flow from Office for the Web and the connected cloud storage, email and authentication services, Microsoft does not offer any choice to administrators or users with respect to the content and volume of the diagnostic data. In the case of the mobile Office apps that provide users with a control for the telemetry level (Word, PowerPoint and Excel), if the administrators have not minimised the telemetry flow, processing is by default set at the highest level (the level Optional). In these apps the Connected Experiences are also enabled by default,

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).

if the system administrators have not centrally blocked the access. Administrators can also completely block access to the government work accounts from the mobile Office apps.

In Office for the Web, system administrators can only disable the Additional Optional Connected Experiences, not the other Connected Experiences. As assessed in section 11.3 of this report, Microsoft as the controller, has no legal ground for the processing of diagnostic data from the mobile Office apps and the Controller Connected Experiences for most of the purposes of its privacy statement. If the government organisations do not block access to the mobile Office apps, they become joint controllers with Microsoft and accountable for the risks of unlawful processing of personal data.

Possible usefulness (nice to have) does not meet the strict requirement of necessity. Via the telemetry events from Office for the Web, Microsoft collects content data. Because Microsoft's role in this processing is unclear, this processing of diagnostic data by Microsoft may disproportionately infringe on the interests and rights of data subjects, in particular as regards confidential data or data of a sensitive nature or special categories of data.

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, AVG). 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, AVG).

As explained in section 10 'Retention periods', Microsoft will retain 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 Microsoft Rijk). Microsoft retains the cloud logs with file and path names and subject lines of mail for 90 days. Microsoft can store the content data that it obtains from the Office for the Web telemetry for 18 months.

It is difficult to argue that such old data are necessary, adequate and relevant for the three or seventeen different purposes for which Microsoft processes the data, depending on its role as processor or as a data controller.

The processing of the diagnostic data by the Controller Connected Experiences and the mobile Office apps, and the processing of the specific content telemetry data from Office for the Web, does not meet the proportionality requirements. This is due to the lack of transparency, the absence of a technical opt-out and the real risk of unlawful further processing of data traffic from the apps by third parties for their own (marketing) purposes.

14.3 Assessment of the subsidiarity

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

Microsoft takes the view that both its Enterprise and individual consumer users choose to make use of its software and services. Microsoft says it makes its software as configurable as possible. End users themselves choose to use the mobile Office apps and choose to share data with third parties such as the helpdesks of UserVoice and Helpshift. According to Microsoft, Enterprise customers are free to determine the nature of the data processing via the Office Cloud Policy Service and/or other specific configuration controls, for example via mobile device management solutions. Microsoft indicates that the configuration options are limited by the flexibility of the platform.

With this point of view, Microsoft assumes that government organisations and the individual employees are free to choose other software. But that freedom is limited in reality. There are no directly comparable software alternatives, other than Google G-Suite or open source software. No public research has yet been done into the privacy risks of, and privacy controls for, the use of such alternative software. As far as Google is concerned, this is also a USA based company, with at least in part the same risks for data subjects, for example with regard to the transfer of personal data to the United States. Even in the event of a potential switch to open source software, the government organisations must first identify the privacy and security risks, and the question whether the software offers the necessary functionalities. In addition, there are switching costs, for example in connection with the conversion of documents made in Office (e.g. templates and track changes that cannot be converted properly without serious loss of usability). In addition, there are costs for migration to new systems and redevelopment of specific applications that are in use with the Office software. This situation is also referred to as vendor lock-in.

An important reason for government organisations to switch to Office 365 licenses (in addition to the fact that Microsoft is discontinuing technical support for older versions of Office, such as Office 2016) is the ability to allow employees and students to work on different devices anywhere in the world, at any time, at home and while travelling. Government organisations cannot influence telemetry from Office for the Web, but they can effectively prohibit the use of the mobile Office apps by blocking access from the apps to the work environment. But in doing so, they would deny employees important functionality of the Office package. As described in Section 5.3.1, Microsoft has explicitly added the use of the mobile Office apps to the Enterprise volume licenses in 2018, precisely so that users can be productive on the road.

In the Online Service Terms of January 2020, Microsoft writes under the heading 'Smartphone and Tablet Devices' that an Office 365 Business or Office 365 ProPlus user may log on to five different smartphones or tablets with the work or school ID. mobile Office apps. As explained in Chapter 5 of this report, Microsoft should act as a data processor for the mobile Office apps. However, this DPIA shows that Microsoft does not comply with the contractual agreement with the Dutch government, and processes diagnostic data as a joint controller with the government organisation. Because Microsoft acts as (joint) data controller for the processing of the telemetry data from the mobile Office apps, and it is difficult to explain to employees why they are not allowed to use the mobile Office apps, the government organisations have no real choice but to offer this functionality.

15. Data Subject Rights

The GDPR grants data subjects a number of privacy rights.

Right to information
First of all, 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 has been highlighted in previous sections of this report, Microsoft does not provide information about the processing of diagnostic personal data through Office for the Web and the Connected Cloud Services, or through the mobile Office apps. Microsoft does not provide this information in a technical language for admins, nor in a clear and simple language for employees or other data subjects whose personal data may be involved in this data processing. As a result, the government organisations, as joint data controllers with Microsoft, are unable to determine whether the processing is lawful in order to adequately inform their employees or students.

Right to access
Secondly, data subjects have a right to access personal data concerning them. Upon request, data controllers must inform data subjects whether they are processing personal data about them. If this is the case, data subjects should be provided 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, 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.*"[214]

As a data processor, Microsoft provides two tools for administrators to search and export all data that Microsoft considers to be a user's personal data. This first tool is the Data Subject Request tool (DSR), the second tool is a self-defined content search query in the audit logs. [215] As described in Sections 2.7 this report, both tools were used to obtain access to information about the use of Office for the Web, the Connected Experiences and the cloud storage and email services. It appears from the results of these access requests for the system-generated log files that Microsoft does not collect many data about the use of the Office for the Web applications, but does collect detailed information about usage of the Connected Cloud Services.

The diagnostic data about Office for the Web do not contain any data about the use of the Connected Experiences at all. This is remarkable, as use was made of different

[214] Microsoft DPA January 2020, p. 7.
[215] There is a third 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.

types of Connected Experiences in the test scenarios, insofar as these were available in the different applications in Office for the Web.

Microsoft equally does not provide access via both tools to the (content) data that it collects via the telemetry messages from Office for the Web. Microsoft considers itself data controller for the processing of data about the use of the mobile Office apps and the Controller Connected Experiences. Microsoft explains that users must send an access request directly to Microsoft, and that Microsoft then responds to the request itself. [216] This can be done via the online (consumer) contact form, under 'Report a privacy concern'. [217]

Privacy Company has sent access requests to Microsoft for all personal data that it had collected as data controller about the two test accounts. As explained in section 2.4, Microsoft confirmed receipt of these access requests, but responded that it had not collected any personal data about the two test accounts. Despite an explanation by Privacy Company that this was not possible, and despite the provision of a number of unique identifiers used during the investigation, Microsoft subsequently refused to grant access.

In sum, when a data subject exercises his rights under the GDPR and requests access to his personal data that Microsoft processes, he can only access the cloud logs about the use of Office for the Web and the Connected Cloud Services via the administrators of his organisation. Via the two tools, Microsoft does not provide access to the log files that Microsoft processes via the Azure Active Directory, access to the telemetry data about the use of the mobile Office apps and Office for the Web or access to the logs it generates about the use of the Connected Experiences, including the Processor Connected Experiences.

This DPIA concludes that Microsoft and the Dutch government organisations are joint controllers for the processing of the telemetry personal data from Office for the Web, the mobile Office apps and the Controller Connected Experiences, if they do not centrally block the access and/or usage. For this reason, the government organisations must agree with Microsoft how and *that* the data subjects can exercise their rights and receive a complete overview and explanation of personal data. Microsoft offers a very good automated tool for DSR, but the results of a request for access should not be limited to the diagnostic data that Microsoft recognises as personal data. The access should also not be limited to the category that Microsoft calls Customer Data, where the displayed data only relate to the cloud services. Even if Microsoft were to grant the requested access to the personal data it processes as a data controller, it would be illogical and unnecessarily burdensome for users to have to address both their own organisation and Microsoft in order to exercise their legal right of access.

Right of rectification and erasure

Thirdly, data subjects have the right to have inaccurate or outdated personal data corrected, incomplete data completed and - under certain circumstances - personal data deleted or the processing of personal data restricted. At present, neither Microsoft nor the government organisations can actually delete historical diagnostic data except for completely deleting the user account.

[216] Microsoft writes: "Part 4 of this guide lists limited scenarios in which Microsoft is the data controller when certain Office 365 products and services are used."
[217] Microsoft writes: "*For all such products and services, your users will need to initiate their own data subject requests directly to Microsoft and Microsoft will fulfill the requests directly to the user."* Microsoft provides a link to https://www.microsoft.com/en-gb/concern/privacy

According to Microsoft it is not possible to delete individual historical diagnostic data, as it is an actual registration of user actions and associated system performance in an ongoing relationship between a customer and Microsoft. Deletion of logs would have significant functional impacts, according to Microsoft, because features that rely on memory (ability to pick up work on another device), would no longer work.[218] Microsoft simply does not want to allow tenants to delete data older than for example 6 months, because system-generated logs are collected per server, not per tenant, and the service is standardised.[219]

It is questionable whether this reasoning meets the requirement of Article 17(1)(a) of the GDPR, which requires a controller to delete the personal data when they are no longer needed for the purposes for which they were collected or otherwise processed or when the personal data have been unlawfully processed (Article 17(1)(d) of the GDPR).

Right to object to profiling
Fourthly, data subjects have the right to object to an exclusively automated decision if it has legal effects. When processing data about the use of Office for the Web, the mobile Office apps and the related cloud services, there are no known decisions that Microsoft makes that have legal consequences or other noteworthy consequences for the rights and freedoms of the data subject. Therefore, this specific right of objection does not apply in this case.

Right to data portability
Employees also have a right to data portability, if their personal data are processed based on the necessity to execute the (labour)contract. As explained in Sections 11.1 and 11.2, this legal ground currently only applies to the processing of Content and cloud logfiles in Office for the Web, the logfiles of the connected Cloud Services, the logfiles of the Azure AD and the Processor Connected Experiences.

Employees are allowed to take their personal data with them, provided that this does not cause a privacy breach with respect to other persons. Such a data transfer may also violate the confidentiality of (government) activities. In that case, the organisations can invoke the exception in article 23 (1) under i of the GDPR.
The individual right to data portability is independent of the possibility that the government organisations themselves must have to move their processing and files collectively to another provider. Microsoft recognises this collective right to portability, as a member of a coalition of North American providers called the Data Transfer Project. Facebook, Google, Microsoft and Twitter are participating in this initiative.

Right to file a complaint
Finally, government organisations as (joint) controllers must inform their employees about their right to complain, internally to the DPO and externally to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

In sum, neither Microsoft nor the government organisations are currently in a position to (fully) honour the rights of data subjects.

[218] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, Answer Q4d.
[219] Ibid, Answer Q4e.

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 Office for the Web and the mobile Office apps. 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 Office applications.

Part D of this DPIA provides an analysis of the remaining risks. Some previously noted risks have already been mitigated by Microsoft in the spring and fall of 2019, as a result of the negotiations with SLM Microsoft Rijk.

16. Risks

16.1 Identification of Risks

The processing of personal data about the individual use of Office for the Web and the mobile Office apps, in combination with the Connected Experiences and the cloud storage services, results in two types of general risks. First, risks through the processing of diagnostic metadata about the use of the services and the software, and secondly, risks resulting from the processing of content data from files, emails and chats for Microsoft's and government's own purposes.

16.1.1 Metadata

Both Microsoft and the government organisations can use the collected diagnostic data about the user behaviour in Office for the Web and the cloud storage services to create a profile of the user. Additionally, Microsoft has access to the user data about the use of the Azure AD, the mobile Office apps and both kinds of Connected Experiences.

As explained in the sections 2.2 and 2.4 of this report, outgoing traffic to third parties has been observed from both Office for the Web and mobile Office apps. Through the mobile Office apps, Microsoft sends personal data to the German company Adjust (through the OneDrive and Outlook apps), and to four US American companies. This latter traffic is sent from the Word app to Cloudflare, from the Outlook app to Helpshift and UserVoice, and from the Teams app to Giphy.

This traffic allows the recipient companies to observe that a unique user, with a unique device ID, has worked with a mobile OneDrive, Outlook or Teams app for a period of time in milliseconds. Although this information in itself does not reveal any sensitive data, the information is transferred to companies in Germany and the USA that are not bound by the privacy guarantees agreed between Microsoft and SLM Microsoft Rijk. According to their own privacy statements, these companies can use the data for their own marketing or analytics purposes. The knowledge that third parties are observing the use of some mobile Office apps, as well as the log-in on the OneDrive website, can also have a negative impact on employees, since these data are not protected by any of the GDPR guarantees and could be traded and/or used for marketing and analytics purposes by the recipients. This risk is assessed in Section 16.2.4.

Although the volume and content of the diagnostic data from the mobile Office apps and Office for the Web are limited compared to the diagnostic data from Office 365 ProPlus (and the Office for the Web telemetry does contain content data, see below in section 16.1.2 Content), the diagnostic data do reveal information about the frequency and exact times of use of the Office for the Web applications and the times and frequency of usage of the mobile Office apps. Microsoft and the government organisations can additionally access the detailed activity logs of the use of the cloud storage and mail services. They can combine these data with log-in and log-out times from the log files from the Azure Active Directory. The diagnostic data about the times of use of the Office for the Web applications and the detailed activity overview of the Connected Cloud Services provide information about the individual log-in behaviour, email behaviour and software usage. Government organisations could use these data for a negative performance assessment of an employee, if such usage is not explicitly prohibited by internal data protection policy rules. The government employees may also feel unable to exercise their right to (moderately) make use of government facilities without being observed and to communicate about private affairs, such as sending an email to a friend or family member. See section 16.2.7.

16.1.2 Content

In its role as data processor for Office for the Web, the Processor Connected Experiences and the Connected Cloud Services, Microsoft collects content data in three different ways.

First, Microsoft collects content data about the use of SharePoint Online, OneDrive for Business, Exchange Online and the Azure Active Directory via its system-generated server logs on its cloud servers. As explained in section 2.5 of this report the content data in the system generated logs may include sensitive or confidential (company) information, and sensitive and special categories of data of all kinds of data subjects, not just government employees. The file and path names may reveal classified or otherwise sensitive / confidential government materials.

Second, Microsoft collects content from the contents of files, emails or chats the moment an end-user uses a Processor Connected Experience, such as a spelling checker.

Last, Microsoft in its role as cloud provider collects every character a user enters and stores in online text, collaboration, presentation and calculation tools (the Customer Data). This last type of content data is outside of the scope of this DPIA. Thanks to the privacy amendment negotiated with Microsoft by SLM Microsoft Rijk in May 2019, the risks of unlawful further processing of these content data by Microsoft have effectively been mitigated.

The only risks the privacy amendment of May 2019 cannot protect against, are requests from law enforcement and secret services/security agencies to get data from Microsoft or its subprocessors, if Microsoft would be prohibited from forwarding such requests to the government organisations and would be prohibited from informing the organisations (*gagging order*). Such access would be in breach of confidentiality requirements and the fundamental right to protection of communication secrecy. Additionally, analysis of the contents of communications could breach government secrecy classifications. The amendment similarly does not protect against unlawful access to the data by a rogue system administrator or hostile state actor. See section 16.2.9 for a more detailed assessment of these risks.
There are other risks related to the possible further processing of these content data by the government organisations. The cloud log files may contain confidential or

organisation sensitive data, such as files names and subject lines of email, and sensitive or special categories of data of all kinds of data subjects, not just about government employees, but also about other recipients of email. There is also a risk of blackmailing and stalking of employees or other licensed users based on these data. Government employees may be inhibited from exercising their legitimate rights, or feel unable to exercise their right to whistle blow.

The knowledge that the government organisations can process these diagnostic content data for profiling purposes can cause a *chilling effect* on employees and other licensed government users of Office. 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.[220]

The data protection authorities in the EU write in their opinion about monitoring on the work floor: *"Technologies that monitor communications can also have a chilling effect on the fundamental rights of employees to organize, set up workers' meetings, and to communicate confidentially (including the right to seek information). Monitoring communications and behaviour will put pressure on employees to conform in order to prevent the detection of what might be perceived as anomalies, in a comparable way to the way in which the intensive use of CCTV has influenced citizens' behaviour in public spaces. Moreover, owing to the capabilities of such technologies, employees may not be aware of what personal data are being processed and for which purposes, whilst it is also possible that they are not even aware of the existence of the monitoring technology itself."*[221]

There is an additional risk for some types of government employees if the logs from for example storage of documents in SharePoint Online reveal that they are regularly working with classified or otherwise government sensitive materials. The employees could become the targets of spear phishing (a scam via email or other electronic communication that is specifically aimed at an individual or organisation), social engineering (an attack technique that exploits human characteristics such as curiosity, trust and greed in order to obtain confidential information or have the victim carry out a certain act) or blackmail.

Therefore, it is essential that access within the government organisations to the metadata is very limited, that access to the metadata is logged and monitored and that government organisations expand their current internal Privacy Statement with detailed rules on the purposes of processing the diagnostic data from all Microsoft products and services (including Windows 10 Enterprise). This risk is described in more detail in section 16.2.7.

Microsoft also collects content data as data controller for the mobile Office apps, the Controller Connected Experiences and the telemetry from Office for the Web. As data controller Microsoft contractually permits itself to process the diagnostic data for a variety of purposes including advertising, product development and product innovation. Microsoft can also use the data for inferred learning, as training sets for machine learning.

[220] Merriam-Webster Online Dictionary, "chilling effect", URL: https://www.merriam-webster.com/legal/chilling effect.
[221] Article 29 Working Party (now: EDPB), WP 249, Opinion 2/2017 on data processing at work, p. 9-10.

Though Microsoft gives the assurance that it processes the information that government employees actively provide via the mobile Office apps and Office for the Web as a data processor after log-in with a work account, this guarantee does not apply to the telemetry data. The telemetry data from Office for the Web contain content data similar to the cloud logs (user, file and pathnames). These risks are described in more detail in section 16.2.1.

Government organisations can mitigate the resulting risks by centrally blocking access to the Controller Connected Experiences. Unfortunately, this opt-out is not yet available or functional for all Office for the Web and mobile Office apps. These risks are described in more detail in section 16.2.3.

16.2 Assessment of Risks

The risks can be grouped in the following categories:

1. Loss of control over the use of personal data
2. Loss of confidentiality
3. Inability to exercise rights (GDPR data subject rights as well as related rights, such as the right to send and receive information)
4. Reidentification of pseudonymised data
5. Unlawful (further) processing

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. [222]

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 Lack of purpose limitation mobile Office apps, Controller Connected Experiences and Office for the Web

As a result of the 2019 negotiations with SLM Microsoft Rijk, if Microsoft is a data processor, it will only process personal data for three authorised purposes, regardless of their origin as Customer Data, as diagnostic data, or system-generated server logs. However, these guarantees do not apply to Microsoft's data processing as data controller. This DPIA shows that Microsoft considers itself to be a data controller for the mobile Office apps.

This DPIA shows that Microsoft considers itself to be a data controller for the diagnostic data from the mobile Office apps and Office for the Web, and the diagnostic data about the use of the Controller Connected Experiences. As controller, Microsoft reserves the right to process the personal data for all 17 purposes of its general privacy statement.

Microsoft is marketing Office 365 as an ecosystem that enables employees to work with all kinds of devices, anywhere. The Dutch government should therefore be able

[222] ICO, How do we do a DPIA?, 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/.

to rely that all data Microsoft obtains through use of the government Office 365 licenses are covered by the new privacy guarantees. An important part of the privacy guarantees agreed upon in May 2019 is the limitation of the data processing to three specific purposes, and only to the extent proportionate.

At the lowest telemetry level 'Neither', Microsoft collects very limited data on the individual use of the services via the diagnostic data on the mobile Excel, PowerPoint and Word apps (as opposed to the telemetry flow from Office 365 ProPlus). The investigation of the mobile Office apps shows that Microsoft does not collect any content data from the content of files, email or chats via the telemetry events, nor any file or path names, when the telemetry is set to the lowest 'Neither'. Due to the relatively innocent content and the relatively small number of diagnostic messages, the impact for data subjects of the lack of purpose limitation in the processing of these diagnostic data appears to be minor.

Nevertheless, the likelihood is high that Microsoft will unlawfully process personal data from the telemetry, because Microsoft, as the data controller, allows itself to process the data for all 17 purposes of its privacy statement. For example, for the unsolicited display of targeted recommendations on the screen to the user.

In response to this report, Microsoft has confirmed that it considers itself the data controller for the mobile Office apps (see paragraph 5.3.1). Microsoft further explained that it only processes Customer Data and personal data from logged in school accounts as a data processor, only for the three agreed purposes. However, this is not correct as Microsoft does not apply the agreed privacy guarantees to the diagnostic data from the mobile Office apps.

As a result, the risks of unlawful processing for purposes other than the three authorised purposes on which the government organisations should be able to rely are more likely than not. This can have negative consequences for the data subjects, for example because Microsoft could send them unsolicited e-mail. That is why the privacy risks for the data subjects are high.

The inspection of the outgoing traffic shows that Microsoft collects substantive data such as user names, file names and pathnames via the new telemetry stream from the browser about the use of Office for the Web. Even though such diagnostic data should fall under the agreed privacy guarantees and Microsoft should only process these data as a processor, it appears that Microsoft allows itself to process these data for all 17 purposes of its general privacy statement. As a result, Microsoft is a joint controller together with the government organisation. Government administrators cannot influence or block this traffic. As this report describes, Microsoft, as the data controller, has no legal ground for the processing of these diagnostic data.

In view of the lack of purpose limitation with regard to these apps and services, as well as the lack of a possibility to centrally prohibit the use of Office for the Web, the risk of occurrence of harm is 100%, while negative consequences for data subjects cannot be excluded. Therefore, this results in a high data protection risk.

16.2.2 Lack of transparency diagnostic data Office for the Web, mobile Office apps, Connected Experiences and Connected Cloud Services

Since May 2019 Microsoft provides a lot of public information about the Office 365 ProPlus telemetry data, and allows users to view the collected data via the Data Viewer Tool. However, Microsoft has not published any documentation about the diagnostic data collected through Office for the Web, the mobile Office apps, the Connected

Experiences and the system-generated event logs about the use of the Connected Cloud Services SharePoint Online, OneDrive for Business, Exchange Online and the Azure AD.

Microsoft is in the process of making the Data Viewer Tool for Windows 10 and Office 365 ProPlus suitable to decode the telemetry messages from a number of mobile Office apps, but the tool only works in the Word, PowerPoint and Excel apps as at the completion of this DPIA on 31 March 2020. The technical inspection of the outgoing data, as described in section 2.2 of this report, shows that Microsoft does not collect any content data from the contents of files, emails or chats nor any file or path names through telemetry data from the mobile Office apps. Therefore, the consequences of this processing for employees can be estimated as low. However, the research also shows that Microsoft sends data from various apps to third parties, without any information about the existence and purposes of this processing (see also Section 16.2.5). Because this traffic is invisible to the end user, users are prevented from exercising their rights, such as filing an objection, asking for deletion and/or access to the data and the profile. The probability of occurrence of this risk is 100%, while the consequences for data subjects are very serious. Preventing access is a violation of a fundamental right of data subjects.

Microsoft also provides very limited information about the personal data it processes via the event logs generated by the system and through the use of Office for the Web, the Connected Experiences and the Connected Cloud Services.

In the logs about the Connected Cloud Services, Microsoft processes e-mail addresses, file and path names, subject lines and addressees, as well as all kinds of specific actions that users perform in those cloud services with documents such as storing, sharing and modifying. Microsoft has not yet published public, centrally accessible and detailed documentation about the diagnostic data it collects through the system-generated log files of its own cloud services. The only way for a data subject to obtain information about the processing of these diagnostic data is by asking the administrator to exercise an access request with the DSR tool, and conduct a search in the audit logs. The lack of public documentation means that data subjects do not have sufficient insight into what information is recorded about their behaviour. As a result, they do not know that they can request access to these data via the administrators. The consequences of this lack of transparency for data subjects are serious. The impossibility of exercising privacy rights leads to a high privacy risk for data subjects.

With regard to the telemetry data Microsoft collects about the use of Office for the Web, it follows from the technical research that these telemetry messages contain content data such as user, file and path names. The fact that Microsoft collects these telemetry data, is not documented. Microsoft does not provide a tool to view this data, and has also explained, in response to this report, that it does not plan to develop such a tool. Due to the lack of transparency, there is a 100% chance that it is impossible for data subjects to exercise their rights. Moreover, there is a non-negligible chance of loss of confidentiality, re-identification of pseudonymised data and unlawful (further) processing if these data are stored in the central Cosmos database just like other telemetry data. Given the nature of the data, the consequences for data subjects can be serious. Therefore, the lack of transparency about the processing of Office for the Web telemetry data also leads to a high risk for data subjects.

16.2.3 Loss of control: telemetry Office for the Web and Controller Connected Experiences in the mobile Outlook, Teams and OneDrive apps

Since the spring of 2019, administrators have been able to select three setting options for the telemetry level in the Enterprise versions of Office 365:

1. Optional
2. Required
3. Neither.

Administrators can also use such a central privacy control for the mobile Excel, PowerPoint and Word apps, but not for the telemetry events from Office for the Web. See figure 11 in section 3.1 of this report. Microsoft has indicated that this option will not become available either, because it only collects telemetry at the 'Required' level. Microsoft does not exclude that it acts as the data controller for these telemetry data and could therefore process the data for all 17 purposes of its privacy statement.

Because Microsoft has confirmed the lack of control for the Office for the Web telemetry, there is a 100% chance that the risk of loss of control will occur. Because Microsoft collects content data through these telemetry data, the lack of an option to minimize the flow can lead to serious consequences for data subjects. Therefore, the privacy risks for data subjects are high.

As a second privacy control, Microsoft offers administrators the ability to centrally disable the Controller Connected Experiences for the Word, PowerPoint, Excel and OneNote apps on iOS and Android. This possibility is not (yet) available for the Outlook, Teams and OneDrive apps. Users cannot exercise this control themselves in these apps either. The processing of the contents of emails or conversations via the Controller Connected Experiences for unauthorised purposes may lead to harm for data subjects (for example if LinkedIn or Bing create an incorrect profile and automatically decide to withhold certain information from the employee). Because Microsoft can process content data via the Controller Connected Experiences for all 17 purposes of its general privacy statement, and government organisations can't centrally block the access in all mobile Office apps, there is a reasonable likelihood for the occurrence of harm. In view of the sensitive nature of the content data that Microsoft can process via the Controller Connected Experiences, there are some to serious negative consequences for the data subjects. Therefore the privacy risks for data subjects are medium to high.

Although the administrators have a technical possibility to centrally prevent access to school accounts from the mobile Office apps, with this option they deny users one of the main advantages of the Office package. Moreover, the government organisations run a real risk of new privacy risks if users circumvent the blockade by using other means.

16.2.4 Loss of control: transfer of personal data from Office for the Web to third parties

Traffic is sent from Office for the Web to two external parties (Giphy and Optimizely). Microsoft believes that this traffic falls outside the privacy guarantees. Because the end-user of Office for the Web has no choice with regard to this external traffic, and the government administrators can only centrally block the traffic to Giphy, there is a 100% chance that the risk occurs of unlawful further processing of personal data by Optimizely. Although Microsoft states that Optimizely is only used prior to logging into the OneDrive for Business webpage with a school or work account, this does not make any difference for the data subjects. After all, they cannot choose whether or not to log on to the web page if they wish to use OneDrive for Business via a browser. The

administrators cannot block this traffic centrally either. Because Microsoft has stated that it does not want to stop "*the careful and balanced use of available web services that make today's web services effective*", it is more likely than not that Microsoft will continue to send traffic to (other) third parties that do not act as subprocessors. This can lead to some or serious negative consequences for data subjects, because the third parties can use the received personal data for their own purposes. Therefore, the privacy risks for data subjects are high.

16.2.5 Loss of control: transfer of personal data from mobile Office apps to third parties

Microsoft sends traffic via the mobile Office apps to five external parties and one party that is mentioned as a subprocessor in Microsoft's overview of Core Online Services, but that Microsoft itself calls a third party. In doing so, Microsoft refers to that company's own privacy statement and terms and conditions (UserVoice). Although in theory the administrators should be able to block traffic to four of these parties centrally (because Microsoft qualifies the traffic to these domains as 'Optional'), administrators themselves must take action to block the transfer of data to these third-party services for their employees and Microsoft has not published any policies to easily block this traffic.

The transfer of personal data to independent data controllers in the US leads to loss of control and confidentiality. This has some negative consequences for data subjects. Because the transfers actually take place, this risk is more likely to occur than not. Therefore, the privacy risks for data subjects are high.

The receiving parties may combine the data about specific data subjects with data received from other sources and process these data for their own purposes. These recipients are not bound by the GDPR if they are not subprocessors of Microsoft, but independent data controllers.

It is more likely than not that Microsoft will continue to send traffic via the mobile Office apps to third parties that do not act as subprocessors. This entails some or serious negative consequences for data subjects, because the third parties can use the received personal data for their own purposes. That is why the privacy risks for data subjects are high.

16.2.6 No access for data subjects

As described in section 2.3, in response to a direct access request, Microsoft has not granted access to the personal data that it processes in its role as the data controller for the use of Office 365. Microsoft has confirmed that it does not provide access to personal data that could be shared by multiple users, such as a device identifier. Nor will Microsoft grant access to personal data that it processes as a processor and personal data that third parties process, because these data would not be Office 365 traffic, but, for example, Windows traffic. Although Privacy Company has provided further explanations, Microsoft has not sent a request for postponement or a rejection.

By not providing access, Microsoft does not enable users to make an informed choice to use the mobile Office apps and the Controller Connected Experiences. Normally, users should find out which third parties have been provided with their data through such an Access request. Now that Microsoft refuses to provide this information, the data subjects cannot exercise their fundamental rights vis-à-vis these third parties, including the absolute right to object to direct marketing and profiling under Article 21 of the GDPR, and the rights of access and deletion.

The impossibility for data subjects to exercise their fundamental privacy rights per definition leads to a high risk. In addition, the processing of personal data about the

use of some mobile Office apps for marketing purposes can lead to major risks and impact for the data subjects, through unlawful further processing of personal data of employees, but also through the re-identification of pseudonymised data by linking unique identifiers from multiple sources. The probability that these risks occur is 100%, now that Microsoft has refused to grant the requested access. That is why the privacy risks for data subjects are high.

16.2.7 Employee monitoring system: chilling effect

As explained in section 16.1.1 (*Metadata*), administrators have access to cloud log files containing information about the use, frequency and exact times of use of Office for the Web. The administrators can also view detailed log files with data about the use of the Connected Cloud Services, in combination with log files about logging in and out of the Azure AD. When combining these sources about individual login and email behaviour and the use of the software, the administrators can gain intimate knowledge of somebody's work patterns and lifestyle. Government organisations could use these data for a negative performance assessment of an employee, if such usage is not explicitly prohibited by internal data protection policy rules. The government employees may also feel unable to exercise their right to (moderately) make use of government facilities without being observed and to communicate about private affairs, such as sending an email to a friend or family member.

The cloud log files may contain confidential or business-sensitive substantive information, such as file names and subject lines of email, and sensitive and special personal data of all kinds, not only of government employees, but also of all kinds of other recipients of, for example, email. There is a risk of blackmailing and stalking of employees based on knowledge from this data. The monitoring of these content data by the administrators can also undermine the possibilities of whistleblowing.

The knowledge that their employer can process these data can have a *chilling effect* on Office 365 users. Microsoft actively offers tools to administrators to make such insights available. Microsoft offers Analytics and Activity Reports in the Microsoft 365 admin center to help employers assess and compare the behaviour of employees. Government organisations can allow employees to use MyAnalytics and Delve. Government organisations can thus use the diagnostic data for a staff monitoring system. Processing for this purpose leads to loss of control, loss of the right to maintain (some) privacy in the workplace and unlawful further processing by, for example, drawing incorrect conclusions from the diagnostic data.

Absent a policy with specific rules about the purposes for which the diagnostic data may be processed, the likelihood of occurrence of these risks is more likely than not. This could well cause *a chilling effect*. Out of fear of being monitored, employees could start to behave differently, be inhibited from becoming a whistle-blower or for example contact certain people. This would not only infringe on their privacy rights, but also impede their exercise of related fundamental rights such as the freedom to send and receive information. Given the dependence of employees of the use of Microsoft products and services at work, they have no means to avoid this monitoring of their behaviour. The consequences for data subjects can be very serious, up to and including wrongful dismissal.

Based on the case law of the European Court of Human Rights[223], government organisations need to expand on their internal privacy policies, and in particular

[223] European Court of Human Rights (Grand Chamber), Bărbulescu v Romenia, 5 September 2017, nr. 61496/08. See in particular the explanation about the assessment criteria in par. 121.

disclose to employees under which circumstances and for which specific purposes these data may be viewed. It is likely that government organisations already have such rules. Therefore, the probability that these risks will occur, can be estimated as very low. Because of this remote chance, even though the impact may be very high, the data protection risks for the employees are low.

16.2.8 Retention period of 18 months: no possibility to remove historical data

The retention periods for diagnostic data at Microsoft are not clear. This results in the risk that data subjects cannot exercise their rights to request inspection or to have obsolete data deleted, for example.
Although Microsoft has published a table of retention periods for Office 365 data, this table is not complete. The table describes how long Microsoft retains data after a customer actively deletes the data, or after a customer terminates the subscription (passive deletion). For example, for an employee who has been employed for more than five years, the retention period would be at least 5.5 years.

However, this table does not provide any insight into the retention period of the audit log files (30, 90 or 93 days after creation) and the retention periods of the telemetry data.

The second DPIA for SLM Microsoft Rijk for Office 365 ProPlus dated 23 July 2019 quotes a letter from Microsoft from which it appears that all diagnostic data are stored for a long period of time, up to 18 months, in the central Cosmos database in the US. It is not possible for users of the software to delete historical diagnostic data per device ID. Customers can only do this by deleting a user account in the Active Directory and then creating a new account for that user.

The GDPR requires that personal data may only be stored as long as necessary for the purposes for which they were collected. The chance that a privacy risk occurs is per definition higher with a long retention period, due to an increased risk of unlawful processing, data becoming inaccurate/outdated and data breaches. Because of the relatively innocent content and the relatively small number of telemetry events from the mobile Office apps and Office for the Web, the impact of this risk for data subjects is low, with the exception of the processing of content data in Office for the Web telemetry. Given that SLM Microsoft Rijk has in any case reduced the retention period to a maximum of 18 months after collection (not after first use of the software) and because possible unlawful processing and re-identification of the limited telemetry data from the mobile Office apps have little to no negative consequences for data subjects, the risks for data subjects are low.

As explained above, this analysis of a low risk of a long retention period does not apply to the content data collected via the Office for the Web telemetry, the data collected through the Controller Connected Experiences, or to the traffic sent to third parties from the mobile Office apps and from Office for the Web. These types of data processing should be prevented all together.

16.2.9 Transfer of personal data to data processor outside of the EEA

As explained in section 7 of this report, the transfer of personal data outside of the European Economic Area (EEA) poses a risk in itself, because the standard of protection of personal data in most countries in the world is lower than in the European Union.[224] As a processor, Microsoft collects detailed information about the behaviour of users in its cloud log files. Section 12.1 describes three general risks for

[224] The GDPR applies in the European Economic Area. This includes the member states of the EU and Iceland, Liechtenstein and Norway.

unlawful further processing of personal data, (i) through orders to Microsoft Corporation from USA law enforcement authorities, security agencies and secret services, (ii) through rogue administrators at Microsoft and at subprocessors, and (iii) through hostile state actors.

While Microsoft undertakes to ensure a uniformly high standard of protection, this protection cannot be guaranteed against government interference of third countries outside the EEA. There is therefore a non-negligible risk that local authorities outside the EU may gain access to the information.

With regard to the risk of hacks through rogue administrators or hostile state actors (or a combination of both), local, *on-premise* hosting does not offer better guarantees for the timely detection of new risks, or for the implementation and monitoring of up-to-date security measures. Microsoft has a very large number of dedicated security staff and controls the legitimacy of access to personal data with regularly audited technical and organisational measures.

As explained in section 7 of this report, Microsoft transfers the diagnostic data from Office for the Web, the Connected Cloud Services and the Processor Connected Experiences to the United States as data processor with the guarantees of the EU Standard Contractual Clauses.

The diagnostic personal data from the Controller Connected Experiences and the mobile Office apps are transferred on the basis of the EU-US Privacy Shield agreement. Microsoft has self-certified its compliance with this privacy regime.[225]

Although both of these transfer mechanisms are legally valid, and approved by the European Commission, there are serious doubts about the future validity of these instruments with regard to transfers to the US. Both instruments are subject to proceedings before the European Court of Justice. The Court has been asked to decide whether these agreements provide sufficient protection against the risks of mass surveillance in the United States. These risks have been revealed by whistle-blower Edward Snowden, also with respect to the interception of data that is still en route (transit traffic).[226]As explained in section 7 the risks of interception of data in transit should not be overestimated.
These risks (of access to personal data by law enforcement, security services and intelligence agencies in the US) do not only apply to the content data stored on Microsoft's cloud servers but also to the diagnostic data, and they apply worldwide.

[225] Microsoft is an active participant in the Privacy Shield Framework https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK&status=Active

[226] In case C-311/18 the European Court of Justice will take the facts into consideration established in the case of Max Schrems versus the Irish DPC (also known as Schrems-2). The court hearing took place on 9 July 2019. Advocate General Henrik Saugmandsgaard Øe has published his Opinion on 19 December 2019. The AG observes that contractual arrangements between parties are very different from the assessment of adequacy by the European Commission in the Privacy Shield agreement with the USA. Data controllers, or DPAs if the data controllers themselves should not intervene, should decide to stop the transfer if there is a conflict between the obligations under the Standard Contractual Clauses and the obligations in the country of destination, such as for example a legal obligation to comply with orders to provide personal data. In practice, this is difficult for data controller in the EU. In case of a gagging order or secret service order they can not know if the recipient is forced to comply with an obligation that conflicts with the Standard Contractual Clauses. The AG does not give advice on the validity of the Privacy Shield, but nevertheless explains why he has doubts about its legal validity. The other procedure is Case T-738/16. This request was filed by the French non-governmental digital rights organisation La Quadrature du Net on 9 December 2016. The hearing at the court was scheduled for 1 and 2 July 2019 but has been postponed in order to allow the court to first decide about the Schrems-2 case.

Although Microsoft provides guarantees regarding the storage of content in data centers in the Netherlands and Ireland, North American courts reserve the right to demand access to these data under the USA CLOUD Act. This Act effectively extends the jurisdiction of North American courts to all data under the control of North American companies, even if that data are stored in data centers outside the territory of the United States.

Microsoft publishes a transparency report twice a year on the number of requests by law enforcement agencies. Microsoft explains that it receives few requests/claims with respect to Enterprise business customers of cloud services.[227] According to the reports on the second half of 2018 and the first half of 2019, the number of requests has almost doubled: from 22 to 42 granted requests for data from Enterprise customers. In the first half of 2019, this concerned 20 requests for metadata and 22 for content data. Of these requests, 15 came from the US. Microsoft does not disclose the origin of the other requests.[228]

Under the OST and DPA, Microsoft is contractually bound to inform its customers if it receives such a request, unless it receives a *gagging* order. Microsoft has explained to SLM Microsoft Empire that there is a high legal threshold for US agencies to issue such a gagging order in case of Enterprise customers.

Although Microsoft also publishes a transparency report about FISA orders twice a year, these reports only contain estimates of totals, not broken down by country or type of customer (consumers or enterprise). [229]

In addition to Customer Data, the system-generated diagnostic data about the use of Office for the Web with the Connected Cloud Services may also contain content data, special categories or sensitive personal data, and secret, classified or confidential information if collected through the use of the Connected Experiences and in filenames

[227] Microsoft explains in its transparency report about requests of enforcement authorities, in reply to the question 'How many enterprise cloud customers are impacted by law enforcement requests': *In the first half of 2019, Microsoft received 74 requests from law enforcement around the world for accounts associated with enterprise cloud customers. In 32 cases, these requests were rejected, withdrawn, no data, or law enforcement was successfully redirected to the customer. In 42 cases, Microsoft was compelled to provide responsive information: 22 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 22 instances that required disclosure of content data, 15 of those requests were associated with U.S. law enforcement.* In the second half of 2018, Microsoft received 61 requests for data of Enterprise customers. 39 requests were rejected or withdrawn.
In reply to the question about the consequences of the CLOUD act, Microsoft writes: "*In the first half of 2019, Microsoft received 4,860 legal demands for consumer data from law enforcement in the United States. Of those, 126 warrants sought content data which was stored outside of the United States. In the same time frame, Microsoft received 43 legal demands from law enforcement in the United States for commercial enterprise customers who purchased more than 50 seats. Of those demands, 1 warrant resulted in disclosure of content data related to a non-US enterprise customer whose data was stored outside of the United States.*" URL: https://www.microsoft.com/en-gb/corporate-responsibility/lerr/.

[228] Microsoft, Microsoft Law Enforcement Requests Report, URL: https://www.microsoft.com/en-gb/corporate-responsibility/law-enforcement-requests-report. For all European customers Microsoft has received 24.175 requests in the first half of 2019, relating to 43.727 people. Microsoft refused 26.76% of these requests, and could not find data in 14.46% of the cases. Compared to the amount of requests for consumers and SME customers, the amount of requests for data from Enterprise customers is still very low, says Microsoft, namely 0.3%.

[229] Microsoft, U.S. National Security Orders Report, URL: https://www.microsoft.com/en-gb/corporate-responsibility/fisa . In the second half of 2018 (last available report) Microsoft received between 0 – 499 orders for content data, relating to 13,500 - 13,999 accounts.

and pathnames when using the cloud storage services. These diagnostic data are also stored in the U.S., with the same risks as described above.

In addition, Microsoft's privacy guarantees regarding the forwarding of law enforcement requests do not apply to the mobile Office apps and the Controller Connected Experiences, as Microsoft considers itself to be the data controller. In its general privacy statement, Microsoft writes that it may share personal information, including content, "*when we have a good faith belief that doing so is necessary to do any of the following: Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies.*"[230]

The risks associated with the transfer of the diagnostic data to a provider outside the EEA are not specific to Microsoft, but apply to all cloud service providers. All cloud service providers must necessarily collect data on the interaction of users with their servers (functional data), and store some of these data as diagnostic data.

As assessed by the European Data Protection Board (EDPB) and the EDPS in their joint opinion to the LIBE Committee of the European Parliament on the CLOUD Act, transfers of personal data must comply with Articles 6 (principles) and 49 (exceptions allowing transfers) of the GDPR. If there is an order on the basis of the US CLOUD Act, the transfer can only be lawful if it is based on an international treaty. The supervisory authorities stress the need for new MLATs (mutual legal assistance treaties) and the need to negotiate an international treaty between the EU and the US on cross-border access to electronic evidence for judicial cooperation in criminal matters.

It is up to the European Court of Justice to assess the validity of the Privacy Shield and the SCC for the transfer of data from the EEA to the US, and up to the European Commission to negotiate a new mutual legal assistance treaty with the US, as well as a treaty on access for investigative services.

It is up to the government organisations to determine what risks they consider acceptable related to the transfer of the diagnostic data to the US. Depending on the sensitivity and confidentiality of the data, they may also decide to use only local storage for some data, or to use only local accounts. Although this DPIA only assesses the risks of the diagnostic data resulting from the use of Office services, and not the risks of the processing of content data by Microsoft, government organisations are advised to consider adding additional encryption to the content data they want to store on Microsoft's cloud servers. As described in section 12.1 Microsoft offers two relevant encryption services for Office 365, namely Customer lockbox and Customer key.

Overall, when using the mobile Office apps, Office for the Web and the Controller Connected Experiences, the likelihood of the occurrence of unlawful access by US courts or agencies/services is remote, while the consequences for data subjects can vary from low to very serious. This results in a low risk for data subjects.

16.3 Summary of risks

These circumstances and considerations as explained above lead to the following five high and four low data protection risks for data subjects:

1. Lack of purpose limitation mobile Office apps and Controller Connected Experiences: loss of control

[230] Microsoft privacy statement, last updated February 2020

2. Lack of transparency diagnostic data: inability to exercise data subject rights
3. Loss of control: telemetry Office for the Web and Controller Connected Experiences
4. Loss of control: transfer of personal data from Office for the Web to third parties
5. Loss of control: transfer of personal data from mobile Office apps to third parties
6. No access for data subjects: inability to exercise data subject rights
7. Employee monitoring system: chilling effects to exercise (related) rights
8. Long retention period: increased risk of reidentification of pseudonymised data and unlawful (further) processing
9. Transfer of diagnostic data to data processor in the USA: loss of control, loss of confidentiality, reidentification of pseudonymised data and unlawful (further) processing

Based on the ICO model, this results in the following matrix:[231]

Severity of impact	Serious harm	Low risk 7,9	High risk 3	High risk 1,2,3,4,5,6
	Some impact	Low risk 7,9	Medium risk 3	High risk 1, 4, 5
	Minimal impact	Low risk 7,9	Low risk	Low risk 8
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm (occurrence)		

[231] 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/

Part D. Description of risk mitigating measures

Following the Dutch government's DPIA model, Part D describes the proposed counter-measures 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 Microsoft, the government organisations and the EU legislator.

17. Risk mitigating measures

In section 16.2 nine privacy risks for data subjects have been discussed. There are six high and three low risks. The government organisations can lower or mitigate some of these risks through technical and organisational measures.

17.1 Measures against the six high risks

Six high risks	Measures government organisations	Measures Microsoft
Lack of purpose limitation for the diagnostic data from mobile Office apps and Office for the Web	Block access to the Outlook, Word, Teams and OneDrive apps from the work accounts on iOS and Android	Only act as processor for the mobile Office apps (except for the Controller Connected Experiences and Microsoft's own legitimate business interests), not as controller, and process the data only for the three authorised purposes
	Discourage log-in to OneDrive via Office for the Web	Only use authorised subprocessors with the Online Services. If Microsoft wishes to engage subprocessors, they must be approved in accordance with the privacy amendment with the Dutch government
	Block traffic from the apps to Giphy, Adjust, Helpshift and UserVoice with group policies	
	Establish policies to prevent file names and path names from containing personal data	Stop sending personal data to third parties unless the third party is an authorised subprocessor or the traffic is approved in connection with an enabled Controller Connected Experience or enabled Add-in and ensure that all Controller Connected Experiences can be centrally turned off by administrators
Lack of transparency diagnostic data Office for the Web, the mobile Office apps, Connected Experiences and Connected Cloud Services	Inform employees of the possibilities for Data Subject Access Requests and access to the audit logs	Publish exhaustive and comprehensible documentation about the processing of diagnostic data from the mobile Office apps, Office for the Web, all

		Connected Experiences and the Connected Cloud Services
	The administrators must regularly use the Data Viewer Tool for the mobile Word, PowerPoint and Excel apps	Make the Data Viewer Tool available for traffic from the Outlook, Teams and OneDrive mobile Office apps and in a similar way give insight in the telemetry from Office for the Web
	As soon as Microsoft makes a tool available to inspect the telemetry from Office for the Web and the other mobile Office apps, use this tool regularly as well	
	Disclose and enforce retention policy / clean up obsolete data	
Lack of control: telemetry level Office for the Web and the mobile Outlook, Teams and OneDrive apps	Retest the new versions of the mobile OneDrive, Outlook and Teams apps	Only act as processor for the mobile Office apps, process the data only for the three authorised purposes
	Recommend users to use the newest versions of these apps when the privacy risks have been mitigated	Implement telemetry choice controls for administrators for the mobile OneDrive, Outlook and Teams apps
	As soon as it is possible: set the lowest telemetry level in mobile Office apps and Office for the Web	Implement the central privacy control for telemetry in Office for the Web
Lack of control: transfer of personal data from Office for the Web to third parties	Discourage log-in to OneDrive via Office for the Web and centrally block traffic to Giphy with group policy	Do not embed services in the Online Services that transfer personal data to third parties, unless the third party is an authorised subprocessor or (part of) an enabled Controller Connected Experience
Lack of control: transfer of personal data from mobile Office apps to third parties	Block access to the mobile OneDrive, Outlook, Teams and Word apps	Do not transfer personal data via the mobile Office apps to third parties if they are not authorised subprocessors
	Block traffic from the mobile Office apps to Giphy, Adjust, Helpshift and UserVoice	
No access for data subjects	Block access to the mobile Outlook, Word, Teams and OneDrive apps	Honour data subject access rights, preferably by expanding the current DSAR tool to include all data collected through the Connected Experiences, Azure AD and mobile Office apps
	Turn off all Controller Connected Experiences	

17.1.1 Measures Microsoft to mitigate high risks

Since June 2019, as a result of the negotiations with SLM Microsoft Rijk, Microsoft has implemented a number of legal, technical and organisational measures to mitigate the risks for data subjects when processing personal data by using Office for the Web and the mobile Office apps.

Technically, Microsoft has made it possible for system administrators to minimise the size of the telemetry events from some mobile Office apps. This option does not yet exist for the commonly used mobile Outlook, Teams and OneDrive apps, nor for the telemetry events from Office for the Web, nor for the diagnostic data that Microsoft stores on its own servers about the use of Office for the Web.

In order to eliminate the six high risks, Microsoft should take the following measures:

1. Only act as data processor for all the services included in the Office 365 licence, including the mobile Office apps and all types of telemetry data, and thus process the data only for the agreed three necessary purposes.
2. Stop sending traffic from Office for the Web and the mobile Office apps to third parties if those companies are not bound by a processing agreement to the three purposes for which Microsoft is allowed to process the data from the Dutch government organisations. The government organisations must be able to grant permission for each subprocessor, for all types of personal data (not just Core Online Services, and not just Customer Data) and from the moment a user uses a service (when installing an app, or when visiting a login page for OneDrive).
3. Publish up to date, detailed, consistent, easily accessible and understandable documentation about the telemetry data Microsoft collects through Office for the Web and the mobile Office apps, and about the diagnostic data Microsoft collects through the cloud service logs, the Azure AD logs and the Connected Experiences.
4. Ensure that administrators can effectively disable use of the Connected Experiences Controller from anywhere, in all mobile Office apps and in Office for the Web.
5. Provide a tool to decipher the telemetry events from Office for the Web and all mobile Office apps.
6. As an intermediate step, until Microsoft acts as processor for all Office 365 Enterprise services: giving the data subjects direct access to the personal data that Microsoft processes as the data controller.

17.1.2 Measures government organisations to mitigate high risks

Government organisations can take a few technical and organisational measures to mitigate these six high data protection risks.

1. Centrally block access to the work accounts from the Outlook, Word, Teams and OneDrive apps on iOS and Android. Alternatively, the organisations should at least create policies to discourage the use of the mobile Office apps for the time being, due to the lack of control over the processing of personal data. This is a temporary stopgap measure, but not an effective one. Due to the lack of purpose limitation, Microsoft can collect and process new types of data for each of the 17 purposes listed in its general privacy statement each time the apps on iOS and Android are updated.
2. Centrally block traffic to Giphy, Adjust, Helpshift and UserVoice and explain to users why they cannot take advantage of the ability to insert images into Teams (both in the app and the online application at Office for the Web).
3. Discourage users from logging in to OneDrive for the Web: it is not possible to centrally block traffic to Optimizely's domains.
4. Turn off the Controller Connected Experiences.

5. Administrators must regularly use the Data Viewer Tool to view the telemetry sent from the Word, Excel and PowerPoint mobile Office apps. As soon as this tool becomes available for the other mobile Office apps, and a similar tool for Office for the Web, administrators should also use this tool regularly.
6. Disclose and enforce retention policy / clean up outdated data due to risks of transfer to the US.
7. Retest new versions of the mobile Office apps / recommend users to install the latest versions as soon as the privacy risks have been mitigated.
8. When using the Connected Cloud Services, establish policies to prevent file names and file paths from containing personal data.
9. Inform employees about the access possibilities via DSR and audit logs.
10. As soon as technically possible: set the lowest possible level for the collection of diagnostic personal data via Office for the Web.

17.2 Measures against the three low risks

Because of the relatively innocent content and the relatively small number of telemetry events from the mobile Office apps and Office for the Web, the risks for data subjects are low. This with the exception of the high risks described above such as the content data found in Office for the Web telemetry data.

There are three low data protection risks. These stem from the lack of transparency, which could make employees think they are constantly being watched, the lack of an effective removal option for historical personal data, and the fact that Microsoft, in its role as processor, processes diagnostic personal data on servers in the United States.

Three low risks	Measures government organisations	Measures Microsoft
Chilling effects employee monitoring system	Complement internal privacy policy employees with specific rules about the use of Office logs by the organisation and by Microsoft	
Retention period of 18 months: no possibility to delete individual diagnostic data	As soon as technically possible: set the telemetry level to the lowest level	Conduct audits on data minimisation and compliance with retention periods
		Data minimisation: create a control for individual deletion diagnostic data without deleting the account
Transfer of (limited amount of) diagnostic data to processor in the USA	Follow guidance from SLM Microsoft Rijk on ECJ Jurisprudence about transfer of personal data to the USA	Consider the creation of an EU cloud
		Data minimisation by improving the privacy controls

17.2.1 Measures Microsoft to mitigate low risks

- Microsoft should offer a control for system administrators to delete some or all diagnostic data of individual users without having to delete the entire account.

Even though Microsoft has announced the end of its German cloud, it should nonetheless consider creating an EU cloud in which not only the Customer Content Data are stored, but also all diagnostic data. At least, Microsoft should move its multi factor authentication servers for the Azure AD to the EU.

17.2.2 Measures government organisations to mitigate low risks

Government organisations can take some additional technical and organisational measures to mitigate the remaining three low risks.

1. Update the existing internal data protection policy with specific information about the purposes and circumstances of the use of, and access to, the Office 365 log files.
2. Follow guidance from SLM Microsoft Rijk about the validity of the Standard Contractual Clauses following jurisprudence of the European Court of Justice. It is up the European Court of Justice to assess the risks of mass surveillance in the USA and up to the EU legislator to mitigate the remaining risks of transfer of diagnostic data from the EU to the USA.
3. Adequately inform employees about the data processing via Microsoft Office 365, what personal data are processed for which purposes, including transfer and processing by third parties or subprocessors.

17.3 Agreed mitigating measures Microsoft

17.3.1 Discussions between SLM Microsoft Rijk and Microsoft following completion of this DPIA

Sections 17.1 and 17.2 discuss the mitigating measures that can be applied by Microsoft and government organisations to mitigate the six high and three low risks for data subjects identified in this DPIA. As discussed in the Introduction of this report, SLM Microsoft Rijk provided Microsoft with the DPIA findings upon completion of this DPIA. SLM Microsoft Rijk and Microsoft then entered into discussions about measures to mitigate the identified high risks. The proposed measures described in section 17.2 formed the basis of these discussions. The discussions between SLM Microsoft Rijk and Microsoft resulted in a set of measures that, upon successful implementation by Microsoft, result in the mitigation of all known high risks. This Section 17.3 describes the agreed measures and explains how they effectively mitigate the identified high risks.

In May 2019, the Dutch government obtained effective audit rights, and will have an independent auditor perform an annual audit to verify compliance with the privacy amendment. A summary of the findings will be published by SLM Microsoft Rijk.

17.3.2 Table with mitigating measures for the six identified high risks

The table below contains an overview of the measures Microsoft has committed to implement that will mitigate the high risks.

No.	High risks	Agreed measures Microsoft
1	Lack of purpose limitation for the diagnostic data from mobile Office apps and Office for the Web	Only act as processor for the mobile Office apps and Office for the Web (except for the Controller Connected Experiences and Microsoft's legitimate business purposes), not as controller, and process the data only for the three authorised purposes
		Only use authorised subprocessors with the Online Services. If Microsoft wishes to engage subprocessors, they will be approved in accordance with the privacy amendment with the Dutch government
		Microsoft will stop sending personal data to third parties unless the third party is an authorised subprocessor or the

		traffic is approved in connection with an enabled Controller Connected Experience or enabled Add-in
		Microsoft will ensure that all Controller Connected Experiences can be centrally turned off by administrators
2	Lack of transparency diagnostic data Office for the Web, the mobile Office apps, Connected Experiences and Connected Cloud Services	Publish exhaustive and comprehensible documentation about the processing of diagnostic data from the mobile Office apps, Office for the Web, all Connected Experiences and the Connected Cloud Services
		Make data viewing capabilities available for traffic from the mobile OneDrive, Outlook and Teams apps
3	Lack of control: telemetry level Office for the Web in the mobile Outlook, Teams and OneDrive apps	Only act as processor for the mobile Office apps, process the data only for the three authorised purposes
		Implement telemetry choice controls for administrators for the mobile OneDrive, Outlook and Teams apps
		Implement technical measures to ensure that diagnostic data collection through telemetry with respect to Office for the Web will be limited to the minimum necessary data
4	Lack of control: transfer of personal data from Office for the Web to third parties	No embedding of services in the Online Services that transfer personal data to third parties via Office for the Web, unless the third party is an authorised subprocessor or (part of) and enabled Controller Connected Experience
		Microsoft will ensure that the third parties identified in this DPIA will either be removed from the service, authorised as a subprocessor, or become (part of) a Controller Connected Experience.
5	Lack of control: transfer of personal data from mobile Office apps to third parties	No embedding of services in the Online Services that transfer personal data to third parties via the mobile Office apps if they are not authorised subprocessors or (part of) and enabled Controller Connected Experience
		Microsoft will ensure that the third parties identified in this DPIA will either be removed from the service, authorised as a subprocessor, or become (part of) a Controller Connected Experience.
6	No access for data subjects	Microsoft will honour data subject access rights where it is a processor by expanding the current DSAR tool to include all data collected through the Connected Experiences, Azure AD and mobile Office apps
		Microsoft will honour data subject access requests for the personal data Microsoft collects as data controller

17.3.3 Remaining mitigating measures government organisations

Government organisations should implement the following measures to mitigate the high risks.

1. Turn off the Controller Connected Experiences.
2. Set the telemetry level of the mobile Office apps to the lowest level.
3. Administrators must regularly use the Data Viewer Tool to view the telemetry sent from the mobile Office apps.
4. Disclose and enforce retention policy / clean up outdated data due to risks of transfer to the US.
5. Retest new versions of the mobile Office apps / recommend users to install the latest versions as soon as the privacy risks have been mitigated.
6. When using the Connected Cloud Services, establish policies to prevent file names and file paths from containing personal data.
7. Inform employees about the access possibilities via DSR and audit logs.

17.3.4 Effects mitigating measures Microsoft

Mitigating measures high risk 1: Lack of purpose limitation mobile Office apps, Controller Connected Experiences and Office for the Web

As detailed in section 16.2.1, the lack of purpose limitation with respect to the mobile Office apps, the Controller Connected Experiences and Office for the Web identified in the DPIA results in a high risk for data subjects.

This high risk is mitigated as follows:
1, At the date of this DPIA report, Microsoft is implementing technical measures to stop collecting content data in the telemetry data from Office for the Web (file, path and usernames), and to ensure that telemetry data collection will be limited to the minimum necessary data.
Microsoft confirmed that it removed historical content data from the Office for the Web diagnostic data.
2. Microsoft will only act as processor for the Office for the Web and the mobile Office apps (except for the Controller Connected Experiences and Microsoft's legitimate business operations) not as controller, and process the data only for the three authorised purposes. authorised

Assuming government organisations follow the recommendation to turn off the Controller Connected Experiences, Microsoft only processes the diagnostic data from Office for the Web and the mobile Office apps for the three authorised purposes. In combination with the commitment from the Dutch government to audit compliance, the risk is mitigated of unlawful processing of data of employees and other data subjects for unauthorised purposes.

Mitigating measures high risk 2: Lack of transparency diagnostic data Office for the Web, mobile Office apps, Connected Experiences and Connected Cloud Services

As detailed in section 16.2.2, the lack of transparency in the processing of diagnostic data in Office for the Web, mobile Office apps, the Connected Experiences and the Connected Cloud Services identified in this DPIA results in a high risk for data subjects.

This high risk is mitigated as follows:
1. Publication of exhaustive and comprehensible documentation about the processing of diagnostic data from the mobile Office apps, Required Service Data from Office for the Web, all Connected Experiences and the Connected Cloud Services.
2. Introduction of data viewing capabilities to view the diagnostic data collected from the mobile OneDrive, Outlook and Teams apps.

3. Microsoft will implement technical changes to the existing Data Subject Access Request tool, that will provide access to the telemetry data collected from Office for the Web and the mobile Office apps, unless providing access would impair the security of the services or would not be legally required.

Microsoft will not provide diagnostic data viewing capabilities for the diagnostic data collected from Office for the Web. However, Microsoft will provide access to the telemetry data from Office for the Web via its existing Data Subject Access Request tool. Microsoft has committed to limit this telemetry collection to the minimum necessary data. Therefore, the lack of transparency for Office for the Web by direct access is sufficiently mitigated by providing access to the collected data to the admins.

Mitigating measures high risk 3: Loss of control: telemetry Office for the Web and Controller Connected Experiences in the mobile Outlook, Teams and OneDrive apps
As detailed in section 16.2.3, the loss of control over the collection of personal data via telemetry in Office for the Web, and through the Controller Connected Experiences in the mobile Outlook, Teams and OneDrive apps identified in this DPIA results in a high risk for data subjects.

This high risk is mitigated by the following measures:
1. At the date of this DPIA report, Microsoft is implementing technical measures to stop collecting content data in the telemetry data from Office for the Web (file, path and usernames). Microsoft will ensure that telemetry data collection will be limited to the minimum necessary data.
2. Microsoft will ensure that all Controller Connected Experiences can be centrally turned off by administrators in Office for the Web and the mobile Office apps.
3. Introduction of data viewing capabilities to view the diagnostic data collected from the mobile OneDrive, Outlook and Teams apps.
4. Microsoft will implement technical changes to the existing Data Subject Access Request tool. This tool will also provide access to the telemetry data collected from Office for the Web and the mobile Office apps, unless providing access would impair the security of the services or would not be legally required.

Microsoft will not make changes to its design of the controls for the different Connected Experiences, and offer the requested clearer choice for system administrators instead of the current three options. Following implementation of the administrator controls for Controller Connected Experiences in all mobile Office apps, and assuming government organisation will follow the recommendation to turn off the Controller Connected Experiences, the risk of unlawful diagnostic data collection through the use of Controller Connected Experiences is sufficiently mitigated.

Microsoft will not provide diagnostic data controls through which government organisations can further minimise the collection of diagnostic data in Office for the Web, equivalent of the level 'neither' in Office 365 ProPlus for telemetry data. Microsoft has agreed to take technical measures to limit the telemetry data collection from Office for the Web to the minimum necessary. Hence, the diagnostic data collection from Office for the Web will only contain relatively innocent identifiers, in a relatively small number of diagnostic messages, and no longer sensitive data such as file, path and usernames. In view of this lack of central telemetry control, this risk still exists. However, assuming government organisations follow the recommendation to turn off the Controller Connected Experiences, the impact of this risk for data subjects is low.

Mitigating measures high risk 4: Loss of control: transfer of personal data from Office for the Web to third parties

As detailed in section 16.2.4, the loss of control through the transfer of personal data from Office for the Web to third parties identified in this DPIA results in a high risk for data subjects.

This high risk is mitigated by the following measures:
1. Microsoft will not embed services in the Online Services that transfer personal data via the mobile Office apps to third parties if they are not authorised subprocessors or (part of) and enabled Controller Connected Experience.
2. Microsoft will ensure that all Controller Connected Experiences can be centrally turned off by administrators.
3. Microsoft will ensure that the third parties identified in this DPIA will either be removed from the service, authorised as a subprocessor, or become (part of) a Controller Connected Experience.

Given these commitments from Microsoft, the effective audit rights and the commitment from the Dutch government to audit compliance, and assuming government organisations follow the recommendation to turn off the Controller Connected Experiences, the likelihood of occurrence of data protection risks must be assessed as remote, while the impact can vary from minimal to serious.

Mitigating measures high risk 5: Loss of control: transfer of personal data from mobile Office apps to third parties

As detailed in section 16.2.5, the loss of control through the transfer of personal data from mobile Office apps to third parties identified in this DPIA results in a high risk for data subjects.

This high risk is mitigated by the following measures:
1. Microsoft will not embed services in the Online Services that transfer personal data via the mobile Office apps to third parties if they are not authorised subprocessors or (part of) and enabled Controller Connected Experience.
2. Microsoft will ensure that all Controller Connected Experiences can be centrally turned off by administrators.
3. Microsoft will ensure that the third parties identified in this DPIA will either be removed from the service, authorised as a subprocessor, or become (part of) a Controller Connected Experience.

Given these commitments from Microsoft, the effective audit rights and the commitment from the Dutch government to audit compliance, and assuming government organisations follow the recommendation to turn off the Controller Connected Experiences, the likelihood of occurrence of data protection risks must be assessed as remote, while the impact can vary from minimal to serious.

Mitigating measures high risk 6: No access for data subjects

As detailed in section 16.2.6, the lack of access identified in this DPIA results in a high risk for data subjects. When Microsoft is a processor, this high risk is mitigated by technical changes to the existing Data Subject Access Request tool, that will provide access to the telemetry data collected from Office for the Web and the mobile Office apps. Microsoft will honour data subject access requests for the personal data Microsoft collects as data controller (i.e. the Controller Connected Experiences) in a similar way through a direct request from the data subject to Microsoft.

Although this measure should ensure that Microsoft, as a processor, will provide access to all personal data required by government organisations to comply with data subject access requests, there is a risk that Microsoft will use the abovementioned exceptions to withhold more data than necessary. This risk also applies with respect to direct data subject access requests to Microsoft where Microsoft is a controller. In such cases, a data subject can always file a complaint with Microsoft's European Data Protection Officer via https://privacy.microsoft.com/en-us/privacy-questions, or, if that would not result in a satisfying reply, with their national Data Protection Authority.

Assuming government organisations follow the recommendation to turn off the Controller Connected Experiences, in combination with the commitment from the Dutch government to audit compliance, the likelihood of occurrence of data protection risks must be assessed as remote, while the impact can vary from minimal to serious.

In sum, Microsoft's technical and organisational measures will mitigate all identified 6 high risks.

17.3.5 *Measures against the 3 low risks following implementation of the mitigating measures*

Section 17.3.4 describes how the high risks identified in this DPIA will be mitigated when the measures have been implemented successfully. This section 17.3.5 describes the 3 low data protection risks and the measures Microsoft and government organisations can take to mitigate these low risks.

The low data protection risks stem from a possible lack of transparency from the government organisations, which could make employees think they are constantly being watched, the lack of an effective removal option for historical personal data, and the fact that Microsoft, in its role as processor, processes diagnostic personal data on servers in the United States.

3 low risks	Measures government organisations	Measures Microsoft
Chilling effects employee monitoring system	Complement internal privacy policy employees with specific rules about the use of Office logs by the organisation and by Microsoft	
Retention period of 18 months: no possibility to delete individual diagnostic data	Where technically possible: set the telemetry level to the lowest level	Conduct audits on data minimisation and compliance with retention periods
	Turn off Controller Connected Experiences	Data minimisation: create a control for individual deletion diagnostic data without deleting the account
Transfer of (limited amount of) diagnostic data to processor in the USA	Follow guidance from SLM Microsoft Rijk on ECJ Jurisprudence about transfer of personal data to the USA	Consider the creation of an EU cloud
		Data minimisation by improving the privacy controls

Conclusions

Since June 2019, as a result of the negotiations with SLM Microsoft Rijk, Microsoft has implemented a number of legal, technical and organisational measures to mitigate the risks for data subjects when processing personal data by using Office for the Web and the mobile Office apps.

Despite these improvements, this DPIA shows that the use of Office for the Web and the mobile Office apps in combination with the Connected Experiences and the Connected Cloud Services still leads to six high and three low data protection risks for data subjects. Some of these risks are new, for example because Microsoft has only recently started collecting telemetry events via Office for the Web, or because Microsoft transfers traffic via the apps and Office for the Web to third parties that are not subprocessors of Microsoft. Other risks are related to the fact that some improvement measures have not yet been implemented effectively. In particular Outlook, Teams and OneDrive are lagging behind.

In order to eliminate the high risks, Microsoft may only act as data processor for all the services included in the Office 365 licence, including the mobile Office apps, and therefore processes the data only for the authorised three necessary purposes. This also means that Microsoft should stop sending traffic to third parties if those recipients are not bound by a subprocessor agreement to the three purposes for which Microsoft is allowed to process the personal data from Dutch government organisations. Microsoft must also publish up to date information about the telemetry data it collects via Office for the Web and the mobile Office apps, and the diagnostic data it collects via the cloud logs, the Azure AD, and the Connected Experiences. Last but not least, Microsoft should provide a tool to decipher the telemetry events from Office for the Web and all the mobile Office apps.

Following completion of this DPIA, SLM Microsoft Rijk and Microsoft agreed upon measures to mitigate the high risks. These measures will be implemented before the end of the summer of 2020 (high risks 1, 4 and 5) and ultimately by the end of 2020. Once implementation has been successfully completed, and assuming government organisations follow the recommendations set out in in this report, all high risks identified in this DPIA will be mitigated. SLM Microsoft Rijk will publish an update on the progress of the implementation of the measures early in 2021.