Ministerie van Justitie en Veiligheid

DPIA Office 365 Online and mobile Office apps (June 2019)

Data protection impact assessment on the processing of diagnostic data

Version 1.1

Date	23 July 2019
Status	Public

Colofon

DPIA by	**Ministry of Justice and Security** **Strategic Vendor Management Microsoft (SLM 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@minvenj.nl T 070 370 79 11
Project name	**DPIA report** diagnostic data processing in Microsoft Office 365 Online and mobile Office apps (June 2019)
Appendices	1. Overview telemetry data observed in iOS and Android apps 2. List of categories of personal data and data subjects
Authors	**Privacy Company** Sjoera Nas, Floor Terra, and Jill Baehring, senior advisors www.privacycompany.eu

CONTENTS

Summary

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 Online). This Data Protection Impact Assessment (DPIA) is about the use of the last two versions of the software: Office Online and the mobile Office apps.

Simultaneously with this report, the Dutch government publishes a DPIA on version 1905 of Office 365 ProPlus, released 22 May 2019 by Microsoft. Both reports take the results into account of negotiations between Microsoft and the Dutch government about contractual and technical improvements.

Outcome: five high data protection risks
The outcome of this DPIA is that there five remaining high data protection risks and four low data protection risks in spite of the contractual, legal and organisational measures that Microsoft has taken to mitigate the data protection risks. These high risks are due to three circumstances:

1. Microsoft acts as a data controller for the mobile Office apps and processes the personal data for all 14 purposes of its (consumer oriented) Privacy Statement. One of these purposes is advertising. At least three of the iOS apps send personal data to a US-based marketing company.
2. Microsoft has not yet built a central opt-out functionality for the Controller Connected Experiences in Office Online and in the mobile Office apps.
3. The government administrators cannot technically prohibit the use of the mobile Office apps.

The risks are described in the two tables below, with suggestions for the measures Microsoft and the government organisations could take to mitigate those risks.

Umbrella DPIA versus individual DPIAs
Negotiations with Microsoft were conducted by the Microsoft Strategic Vendor Management office (SLM Rijk Microsoft). 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 Online and the mobile Office apps, in combination with the use of Connected Experiences and cloud storage services. 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 servers and via the telemetry client in the mobile Office apps. Similar to the telemetry client in Windows 10, Microsoft has programmed the installed versions of the Office software to systematically collect

telemetry data on the device, and regularly send these to Microsoft's servers in the USA.

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
Privacy Company has carried out technical research into the data processing via the mobile Office apps and has managed to decode large parts of the data. The Data Viewer Tool that Microsoft provides for Windows 10 and Office 365 ProPlus cannot be used to decode the telemetry events from the mobile Office apps.

In order to also gain insight into the data that Microsoft processes on its own servers regarding the individual use of Office Online and the cloud storage and e-mail services, data subject access requests were filed with Microsoft, as defined in Article 15 of the GDPR, after having performed scripted scenarios.

The technical analysis of the data from the mobile apps and the results of the data subject requests show that Microsoft collects directly identifiable personal data, such as the user name and e-mail address and the times at which individual employees have performed actions in the applications. Microsoft does not collect many diagnostic data about the use of the mobile Office apps and Office Online, and no content data from the contents of files, e-mail or chats, nor any file or path names. However, when government organisations use the cloud storage and email services SharePoint Online, OneDrive for Business and Exchange Online, Microsoft does collect content data on the titles, pathnames and subjects of files or mails from its system-generated event logs.

The captured network traffic shows that at least three of the Office apps on iOS (Word, PowerPoint and Excel) secretly send diagnostic data to a US-based marketing company, without providing any information about the existence and purposes of this data processing. Although the information when a unique user has worked with a specific application itself does not reveal any sensitive data, the information is transferred to a company in the USA that is not bound by any of the privacy guarantees from Microsoft. The company is specialised in creating predictive profiles of individuals for commercial purposes.

Many mitigating measures Microsoft do not apply to Office Online and the mobile Office apps
The DPIA about the data protection risks of the processing of diagnostic data from Office 365 ProPlus shows that, as a result of the negotiations with SLM Rijk, there are no more known high data protection risks for Dutch government organisations. However, many of these technical and organisational measures are not implemented for Office Online, while the measures do not apply at all to the mobile Office apps.

Microsoft has not created a central technical opt-out for government administrators to prohibit the use of the Controller Connected Experiences through Office Online (or the mobile Office apps).

Microsoft qualifies itself as a data controller for the mobile Office apps. This means that the contractual improvements negotiated by SLM Rijk for Microsoft in its role as data processor do not apply. Microsoft contractually permits itself to process the

data from the mobile Office apps for all 14 purposes from its general Privacy Statement, including advertising and research, even though Microsoft also guarantees that all privacy guarantees effectively apply to all data that are processed from users that are logged in with their Azure Active Directory account.

Since May 2019, Microsoft offers most of the indispensable Connected Experiences such as the Editor (spelling checker) from a role as data processor, instead of as data controller. Nonetheless, there are 14 remaining Controller Connected Experiences.

Microsoft optional Controller Connected Experiences

3D Maps	Researcher
Insert online 3D Models	Smart Lookup
Map Chart	Insert Online Pictures
Office Store	LinkedIn Resume Assistant
Insert Online Video	Weather Bar in Outlook
PowerPoint QuickStarter	Giving Feedback to Microsoft
Research	Suggest a Feature

When government organisations allow their employees to use the mobile Office apps and the Controller Connected Experiences, they become joint controllers with Microsoft for the diagnostic data processing. As a result, the government organisations can be held accountable for the risks that data subjects run with regard to the unlawful processing of their personal data.

Additionally, Microsoft has not published any documentation about the diagnostic data from the mobile apps or Office Online and does not allow administrators to choose a (minimum) level of telemetry.

Risks and mitigating measures

Currently, the processing of diagnostic data about the use of Office Online and the mobile Office apps in the Enterprise environment, in combination with the use of the Controller Connected Experiences, leads to five high data protection risks, and four low data protection risks for data subjects.

No.	High risk	Measures to be taken by Microsoft
1	Lack of transparency	Public documentation about diagnostic data mobile apps and Controller Connected Experiences
		Enable data viewer tool for the mobile apps
		Enable data subjects to exercise their GDPR rights regarding Controller Connected Experiences and mobile Office apps
2	No technical opt-out Controller Connected Experiences and mobile Office apps	Temporary solution: technically prevent data subjects from using the mobile apps in the Enterprise environment OR do not ask for the consent (and cease processing diagnostic data outside of the Azure AD).
		Permanent solution: become a data processor for the mobile Office apps in Enterprise
		Create a central opt-out for data controllers to prevent use of the Contr. Connected Experiences via Office Online and the apps.

No.	High risk	Measures to be taken by Microsoft
3	Unlawful collection and storage of sensitive categories of data through Controller Connected Experiences	Become a data processor for the mobile apps + central opt-out for Contr. Connected Experiences + exclusion of processing for the purposes of profiling, data analytics, market research, or advertising
4	Lack of purpose limitation mobile Office apps and Controller Connected Experiences	Become a data processor for the mobile apps + exclusion of processing for the purposes of profiling, data analytics, market research, or advertising
5	Not enough control over sub-processors and factual processing	Ensure effective audit rights for the Dutch government regarding mobile Office apps and Controller Connected Experiences

The government organisations can take very few effective measures to mitigate the high data protection risks.

1. Establish a policy to warn employees not to use the mobile Office apps and the Controller Connected Experiences
2. Inform employees about their access rights with regard to diagnostic data collected by Microsoft via DSR and the audit logs
3. As soon as technically possible: turn off the Controller Connected Experiences

No.	Low risk	Measures to be taken by Microsoft
6	No control over volume and nature diagnostic data	Offer technical data minimisations choices for diagnostic data in all Office 365 services (not limited to ProPlus)
7	Chilling effects personnel monitoring system	Data minimisation, privacy by default settings
8	Long retention period of diagnostic data	Become a data processor for the mobile apps + central opt-out Contr. Connected Experiences
		Provide documentation about the different retention periods of all diagnostic data
9	Transfer of (limited amount of) diagnostic data to the USA	Data minimisation + become a data processor + effective audit rights. See par 7 and 16.8.2 for measures that should be taken by the European legislator

The government organisations can take a few technical and organisational measures to mitigate the remaining low data protection risks.

1. Update the existing employee privacy policy with specific information for what purposes, and under what circumstances, the organisation may access the different diagnostic data from Microsoft's different services and products
2. Perform DPIAs before using analytical services based on the diagnostic data
3. As soon as technically possible: select the lowest, minimum level for the collection of diagnostic data
4. Support SLM Rijk in assessing the validity of transfer mechanisms after future 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.

Conclusions

Currently, the processing of diagnostic data about the use of the mobile Office apps and the Controller Connected Experiences leads to five high data protection risks. Only Microsoft can effectively mitigate these risks. The government organisations are advised to create policies for their employees to not use Office Online and the mobile Office apps. SLM Rijk will continue its negotiations with Microsoft to ensure that Microsoft realises the negotiated improvements for all services included in the Office 365 license.

Introduction

This report, commissioned by the Microsoft Strategic Vendor Management office (SLM Rijk[1]) of the Ministry of Justice and Security, is a third data protection impact assessment (DPIA) on the processing of personal data about the use of the Microsoft Office 365 software. The Office 365 licenses include 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 Online). This DPIA is about the last two versions of the software: Office Online and the mobile Office apps.

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 large-scale processing of personal data is concerned. The assessment is intended to shed light on, among other things, the specific processing activities which are carried out, 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 tackle 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.[2]

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

[1] SLM is the abbreviation of the Dutch words Strategisch Leveranciersmanagement Microsoft.
[2] *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.

independent administrative authorities.[3] The Microsoft Office software is not new. However, 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.[4]

In GDPR terms SLM Rijk **is not the data controller** for the processing of diagnostic data via the use of the Office software. 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 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 Rijk
Simultaneously with this DPIA about Office Online and the mobile Office apps, SLM Rijk also publishes two DPIAs on the risks of the processing of diagnostic data via Windows 10 Enterprise and Office 365 ProPlus.[5]

The role of SLM Rijk is not limited to Microsoft Office. As representative of all the procuring government organisations, SLM 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 Rijk during the review of the risks of the use of these products.

In the volume licensing agreements, Microsoft releases new versions of its Office 365 ProPlus and Windows Enterprise software twice per year. As part of its ongoing commitment to ensure GDPR compliance, SLM Rijk intends to regularly commission new DPIAs on new versions of Windows 10 and Office 365, to guarantee the rights of data subjects on ongoing basis. New DPIA's 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.

[3] Source: Microsoft Business and Services Agreement, Amendment ID CTM, May 2017, last amended 10 May 2019.
[4] 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.
[5] Website Strategisch Leveranciersmanagement Microsoft Rijk (SLM Microsoft), URL: https://www.rijksoverheid.nl/documenten/publicaties/2018/11/12/strategisch-leveranciersmanagement-microsoft-rijk-slm-microsoft

In November 2018 SLM Rijk has published a first DPIA on the data protection risks of the autumn 2018 version of Office 365 ProPlus, version 1708.[6] The report was published on the Dutch government website with an update on the negotiations between the Dutch central government and Microsoft about the GDPR compliance.[7]

Simultaneously with the DPIAs on Office 365, SLM Rijk has 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 Rijk has 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.[8]

Outside the scope
This DPIA assesses the risks of data processing about the use of the five core apps (Word, Excel, Outlook, PowerPoint and Teams) in the mobile Office apps and in Office Online, in combination with the Connected Experiences (such as the spelling checker) and use of the Microsoft cloud and email storage services SharePoint Online, OneDrive for Business and Exchange Online, a so called *hybrid* set-up (see paragraph 8 of this report).

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

The Microsoft Office 365 licenses purchased by government organisations include other Microsoft cloud services such as Skype for Business, Planner, Power BI, EOP/ATP and Intune. These services also fall outside the scope of this DPIA report.

Technical analysis of the diagnostic data
Privacy Company has applied two different research methods: intercepting and decoding the data traffic from two (brand new and top of the line) smartphones, and retrieving the diagnostic data about the use of Office Online via data subject access requests as referred to in Article 15 of the GDPR.

Privacy Company has used specific test scenarios for the five apps that are expected to be used most frequently (Word, Outlook, Excel, PowerPoint and Teams). In each of the apps additional online services were used, such as the Editor (spelling checker), Translator (translation module) and the insertion of a picture from the Internet (Insert Online Pictures). Since May 2019, Microsoft calls these extra online services 'Connected Experiences'. The scenarios were written in order to reproduce the everyday actions of a government employee. The scenarios were executed on 7 and 8 May and repeated on 7 June 2019. Some specific test scenarios were

[6] 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.
[7] Ibid.
[8] https://www.privacycompany.eu/

repeated on 23 July 2019, to reproduce the findings with regard to traffic from the iOS apps Excel and PowerPoint.

Privacy Company has ensured that the research is reproducible and repeatable. This has been 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 were taken of all actions. All data have been recorded. The captured telemetry messages are shown in **Appendix 1** to this report.

Data subject access requests
When an employee uses Office Online, the entire data processing takes place on Microsofts cloud servers. There is no diagnostic data flow that can be intercepted for inspection from the end-users' devices to or from Office Online. It is equally impossible to inspect via traffic interception how Microsoft processes diagnostic data about the use of the Connected Experiences, SharePoint Online/OneDrive for Business and Exchange Online.

For this reason, Privacy Company has filed (automated) data subject access requests as referred to in Article 15 of the GDPR and created audit log files relating to the activities performed by the investigators. Microsoft offers a dedicated Data Subject Request tool to administrators for this purpose.

Microsoft does not show update data or version history for Office Online. Privacy Company has used the version that was available on 6 May 2019 via the Office 365 license and performed the tests on an Acer laptop with operating system Windows 10 Pro version 1803 and the browser Mozilla Firefox 67.0.2 (64 bits).

Intercepting telemetry traffic
Privacy Company has tested the Office mobile version 2.25 (Word, Excel), 1.0.75 (Teams), 3.21.0 (Outlook) and 10.64 (PowerPoint) on an iPhone X with iOS version 12.2. The same tests were performed on an Android device, Pixel 3, with Android operating system 9. The following versions of the apps were tested: Excel 16.0.11601.20074, Outlook 3.0.55, PowerPoint 16.0.11601.20074, Teams 1416/1.0.0.2019042206 and Word 16.0.11601.20074. During the third run, on 23 July 2019, on the same iPhone X with iOS version 12.3.1, Excel and Word versions 2.27 were tested, as well as version 2.25 of PowerPoint.

Privacy Company has 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
- Login with an Office365 account as needed[9]
- Execute the scripted scenario. Take screenshots of each step.
- Once the script is completely executed, stop the Mitmproxy.

Privacy Company has saved the log files and compared the network endpoints with the limited public information that Microsoft publishes about them. Microsoft only

[9] In most cases, another application was already logged in and used automatically in the other applications.

publishes two lists of network endpoints for Windows, not for Office. [10] However, both Windows lists, for the Windows consumer and professional versions, and for the Windows Enterprise versions, contain network endpoints for Office diagnostic data, such as onecollector.cloudapp.aria, v10.events.data.microsoft.com and watson.telemetry.microsoft.com.

In the network traffic, two endpoints can be identified as telemetry endpoints: vortex.data.microsoft.com and mobile.pipe.aria.microsoft.com. The first endpoint was observed only from PowerPoint on iOS, not from other applications and not from
Android. Only these data were packaged as JSON messages. These data are relatively easy to read in a database.

The data sent to the other endpoint, mobile.pipe.aria.microsoft.com, was encrypted in an undocumented binary format. The raw data were searched in a structured way using specific search scripts, partly based on the content of the test scenarios.

Response Microsoft
SLM Rijk has asked Microsoft to comment on the findings with regard to the mobile apps: the traffic to marketing company Braze and the legal assessment that Microsoft is a data controller for the mobile Office apps. Microsoft has replied by e-mail of 19 July 2019. Microsoft has confirmed that it considers itself to be a data controller for the mobile Office apps, but Microsoft also guarantees that all privacy guarantees effectively apply to all data that are processed from users that are logged in with their (government) Azure Active Directory account. The specific answer is included in paragraph 2.2 of this report.

In response to the finding that there is no technical possibility to block the Controller Connected Experiences from Office Online and the mobile Office apps, Microsoft has referred to the announcement in the documentation about Office 365 ProPlus telemetry data that it will make further improvements, amongst others in the mobile apps.

Microsoft writes: "*We will be extending these new and improved privacy controls to additional Office clients, including Teams, Office for Mac, and our mobile 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.*"[11]

Outline
This assessment follows the structure of the *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017).[12] This model uses a structure of four main sections, which are reflected here as "parts".

A. Description of the factual data processing
B. Assessment of the lawfulness of the data processing
C. Assessment of the risks for data subjects
D. Description of mitigation measures

[10] Microsoft, Windows endpoints non-enterprise editions, URL: https://docs.microsoft.com/en-us/windows/privacy/windows-endpoints-1903-non-enterprise-editions and Windows 1903 Enterprise endpoints, URL: https://docs.microsoft.com/en-us/windows/privacy/manage-windows-1903-endpoints.
[11] Microsoft, Overview of privacy controls for Office 365 ProPlus, last updated 6 May 2019, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/overview-privacy-controls (website last visited and recorded on 8 July 2019).
[12] The Model Data Protection Impact Assessment federal government (PIA). For an explanation and examples (in Dutch) see: https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia

Part A explains the data processing by Office Online 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 negotiations with SLM 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 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 Office diagnostic data processing

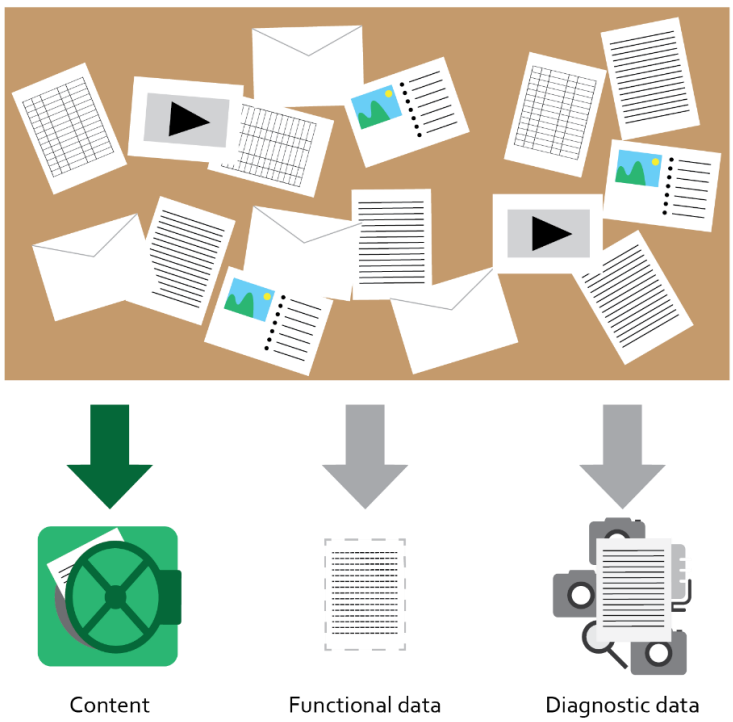
This first part of the DPIA provides a description of the characteristics of the diagnostic data collected via the use of Office 365 ProPlus software. This starts with a short description of the processing of different kinds of data (content, diagnostic data and functional data).

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 general risks caused by the processing of personal data *about* the use of Office Online and the mobile Office apps, in combination with Connected Experiences and the use of SharePoint Online and OneDrive for Business. In this report these data *about the use of the software* are called diagnostic data. They 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.

Illustration 1: Content data, functional data and diagnostic data



In this report, all data about the individual use of the mobile Office apps, Office Online, the use of the 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.

Microsoft uses different terminology and offers different protection to different classes of data. However, for the purpose of analysis and following the logic of ePrivacy law in Europe, this DPIA chooses to group the different kinds of data in these three broad groups.

1. Contents of communication with Microsoft's services, part of 'Customer Data' as defined by Microsoft
2. Diagnostic data, all observations stored in event logs about the behaviour of individual users of the services
3. Functional data, which should be immediately deleted or anonymised upon completion of the transmission of the communication.

Microsoft uses the term Customer Data to refer to all content data that are actively provided by users when using the online services. Most of Microsoft's contractual privacy guarantees relate to these 'Customer Data'. According to Microsoft's Online Service Terms, "*Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. (…)*"[13] Microsoft has provided the following examples of Customer Data: *Customer password, content of customer's email account or Azure data base, email subject line, Machine learning built models with data that is unique to a customer, and email content*. The Customer Data include the subject lines of e-mail and the content data that are collected as part of Connected Experiences such as the spelling checker.

In this report, the term functional data is used for all data that are only necessary for a short period of time, to be able 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 e-mail server, and the data stream necessary to allow the user to authenticate or to verify if the user has a valid license. According to the distinction between the three categories of data made in this report, functional data may also include the content of text you want to have translated. In that case, Microsoft may collect the sentence before and after the sentence you mark for translation, to provide a better translation. The key difference between functional data and diagnostic data as defined in this report, is that functional data are and should be transient.[14] As long as Microsoft doesn't store these functional data, or only collects these data in a strictly anonymous way, they are not diagnostic data.

[13] Microsoft Online Service Terms, July 2019, p. 4. Microsoft also publishes a different definition, in the Microsoft Trust Center, *How Microsoft categorizes data*, URL: https://www.microsoft.com/en-us/trustcenter/privacy/how-Microsoft-defines-customer-data (site last visited and recorded on 8 July 2019). In this definition the Professional Services are excluded. *Customer Data are all data, including text, sound, video, or image files and software, that you provide to Microsoft or that is provided on your behalf through your use of Microsoft enterprise online services, excluding Microsoft Professional Services. For example, it includes data that you upload for storage or processing, as well as applications that you upload for distribution through a Microsoft enterprise cloud service*

[14] 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***

Microsoft uses different words and classifications. The term 'diagnostic data' for Microsoft refers to the specific telemetry data collected by Office 365 ProPlus about the use of the Office software. Microsoft does not have an overall category for the metadata that are generated on its servers by the individual use of the services and software, such as the telemetry data from the mobile Office apps and other metadata generated about the usage of servers in server logs.[15]

In practice most government employees use the Microsoft Office software on devices with the Windows 10 Enterprise operating system. The Windows 10 telemetry client regularly collects event data about the use of apps on the device, including about the use of the Office 365 ProPlus software. The diagnostic data collection from Office 365 ProPlus is separate from, and independent of, the telemetry data stream generated by Microsoft Windows 10.

1.1 About Microsoft Office Online, the mobile apps and the Connected Experiences

The Microsoft Office software includes some of the most popular and most widely-used computer programmes to help people send e-mails, write, calculate, present, chat, collaborate and organise work tasks. As it may be expected that all readers are familiar with the Office products this report will not provide an explanation of the functionality of these programmes and services.

From within the Office applications users can access Connected Experiences such as the spelling checker (Editor), the possibility to insert a picture from the internet or use the translator module. Before May 2019, Microsoft called these services Online Services or Micro services.

These Connected Experiences require that the device has a connection to the internet and can communicate with the Microsoft servers. The Connected Experiences are served in two flavours: either included, or optional. In May 2019, Microsoft has done a major reshuffle of the Connected Experiences. Microsoft now acts as a data processor for the most widely used and indispensable Connected Experiences, such as for example the spelling checker (Editor), Translator, insert pictures from the internet, handwriting to text and PowerPoint Designer.

Only 14 services of the 63 Experiences remain 'optional'.[16] In case the use of a Connected Experience is optional, the individual end-user is shown a consent request from Microsoft the first time he or she wants to use such a Connected Experience (see paragraph 3.2 in this report *Privacy choices in Office Online and the mobile Office apps*). In that case the data processing is not governed by the data protection rules set by the agreement between Microsoft and SLM Rijk. As will be described in paragraph 5 of this DPIA *Roles: Data controller, data processor and sub-processor*, Microsoft considers itself to be a data controller for the use of optional Connected Experiences and contractually permits itself to process the resulting personal data for its own purposes, as outlined in its Privacy Statement.

***traffic management purposes**, and that during the period of storage the confidentiality remains guaranteed."*

[15] Slides presented by Microsoft on 1 November 2018.

[16] Microsoft, Connected Experiences in Office, URL: https://support.office.com/en-us/Article/connected-experiences-in-office-8d2c04f7-6428-4e6e-ac58-5828d4da5b7c?ui=en-US&rs=en-001&ad=US . Microsoft complete list of services (Connected Experiences): https://docs.microsoft.com/en-us/deployoffice/privacy/connected-experiences. Microsoft overview of the optional (Controller) Connected Experiences: https://docs.microsoft.com/en-us/deployoffice/privacy/optional-connected-experiences (all three websites last visited and recorded on 8 July 2019).

Microsoft optional Controller Connected Experiences

3D Maps	Researcher
Insert online 3D Models	Smart Lookup
Map Chart	Insert Online Pictures
Office Store	LinkedIn Resume Assistant
Insert Online Video	Weather Bar in Outlook
PowerPoint QuickStarter	Giving Feedback to Microsoft
Research	Suggest a Feature

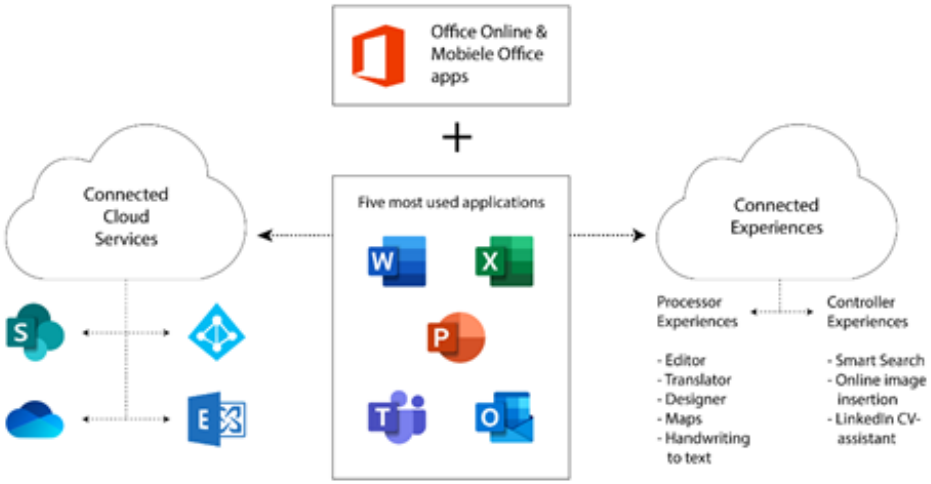
Microsoft Office can be installed in different ways, purely local, or in a combination with Microsoft cloud services (*hybrid deployment*). The current ways in which the Dutch government deploys the software, including the pilot with the use of SharePoint Online and OneDrive for Business, are described in paragraph 8 of this report, *Techniques and methods of data processing*.

1.2 Scope

The aim of this DPIA is to assess whether and how Office Online and the mobile Office apps can be deployed in a GDPR compliant manner by government organisations in relation to the processing of data about the usage of the software. This report occasionally refers to the other DPIA report about Office 365 ProPlus for SLM Rijk that is published simultaneously with this report.[17]

This report specifically assesses the mitigating measures implemented by Microsoft to ensure that the processing of personal data related to the use of the online services, such as Office Online and the cloud storage and e-mail services (SharePoint Online, OneDrive for Business and Exchange Online), can be done in accordance with the GDPR, what the available privacy options are for the organisations that will use the software, and what the (remaining) risks for the privacy of the users may be.

Illustration 2: Assessed Office 365 services and applications



The scope is limited to the processing of diagnostic data by the five main applications provided in Office: Outlook (including Calendar functions), Word, Excel

[17] Rijksoverheid, URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/?.

PowerPoint and Teams. This DPIA also addresses the risks of opening and storing documents in SharePoint online, and the risks caused by the use of a few specific Connected Experiences.

Out of scope
This DPIA is limited to an analysis of the data protection risks caused by the use of Office Online (Microsoft cloud based apps accessed through a browser) and the mobile Office apps that can be installed on mobile devices with iOS and Android operating systems. This data protection risks of the diagnostic data processing through Office 365 ProPlus (the installed version of the software) are subject of a separate DPIA that is published simultaneously with this DPIA by SLM Rijk.

This report describes the diagnostic data that result from the storage and retrieval of documents in SharePoint Online, OneDrive for Business and Exchange Online, but no other types of storage in the Microsoft cloud. The Dutch government mainly stores content data in its own data centres (on-premise).

In practice most government employees use an installed version of the Office software on devices with the Windows 10 Enterprise operating system. Additionally, they can use Office Online and the mobile Office apps on mobile devices. The Windows 10 telemetry client regularly collects event data about the use of apps on the device, including about the use of the Office software. There could be an additional or higher risk if the Windows 10 telemetry data were combined with the separate diagnostic data collected about the use of the Office software. This report however assumes that all government organisations follow the recommendation to set the level of telemetry to minimum, to the *Security* level, thus preventing Microsoft from capturing rich events about the use of the different Office applications.[18]

Microsoft writes: "*We will be extending these new and improved privacy controls to additional Office clients, including Teams, Office for Mac, and our mobile 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.*"[19]

This DPIA does not describe the specific deployments chosen by the different government organisations that procure the Office software (see paragraph 8 in the DPIA). In Microsoft terminology, the government organisations are called *tenants*. It is up to these *tenants* to assess the specific risks caused by their specific types of personal data and types of data subjects affected by the processing of diagnostic data. This DPIA can only provide a general overview of the risks and different available privacy settings and options for the *tenants* and the end-users.

This report provides a snapshot of the current data protection risks. Microsoft can dynamically add new events to the diagnostic data stream, and can add new functionality. Outside developments may also influence the assessment, such as judgments from the European Court of Justice, or negotiations between the European Commission and the United States about a mutual legal assistance treaty.

[18] DPIA report for SLM Rijk on the diagnostic data processing via Windows 10 Enterprise, URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/Samenvatting+DPIA+Windows+10+Enterprise+11+juni+2019.pdf.
[19] Microsoft, Overview of privacy controls for Office 365 ProPlus, last updated 6 May 2019, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/overview-privacy-controls (website last visited and recorded on 8 July 2019).

1.3 Visibility diagnostic data for end-users

Microsoft systematically collects data about the use of its software. With the installed versions of the software, be it on a laptop or on a tablet or on a smartphone, it does this via a built-in telemetry client. This software records all kinds of actions that a user performs on the device and regularly sends the data, in batches, to Microsoft's servers in the United States. These diagnostic data are transmitted in unknown binary format. This applies to Windows 10 Enterprise, but also to Office ProPlus and the mobile Office apps.

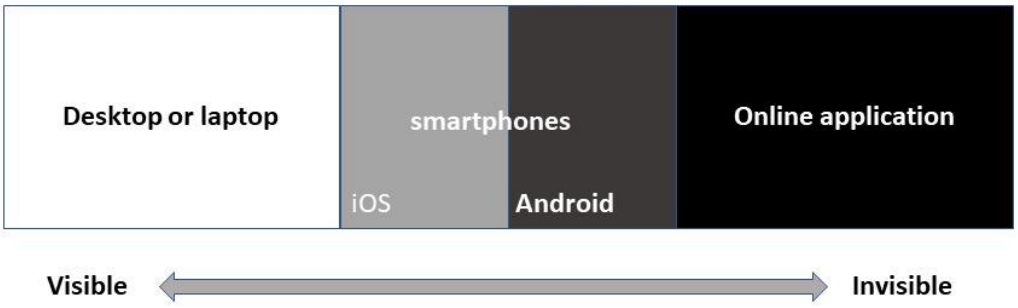
In the new versions of Office 365 ProPlus released after 29 April 2019, end-users can see the contents of telemetry data collected via the telemetry client in Office 365 ProPlus via the Data Viewer Tool. Unfortunately, this tool is not available for the diagnostic data from the mobile Office apps.

On the mobile devices, Microsoft has less control over the operating system (in this report limited to iOS and Android). Telemetry events about individual use are sent to Microsoft, but less than from the fixed equipment. Users cannot see this traffic via the Data Viewer Tool, since this tool is built for devices with Windows as operating system. Privacy Company has performed test scenarios on two smartphones, intercepting the data and decoding it as adequately as possible.

The operation of the telemetry client in the mobile Office applications is not consistent. For example, the PowerPoint app on iOS sent telemetry in a (relatively easy to read) JSON format during the tests, while all other apps, and all apps on Android send messages in an undocumented binary format.

In the online applications, which run in a user's browser, Microsoft collects personal data about the use of the applications in log files on its own cloud servers. Microsoft records these diagnostic data in so-called system-generated event logs. This applies not only to the data about the use of Office Online, but also to diagnostic data about other Microsoft online services such as the Connected Experiences, Azure Active Directory, SharePoint Online and OneDrive, and the cloud mail server Exchange Online.

Illustration 3: Visibility diagnostic data Microsoft Office for end-users



In order to see the contents of the diagnostic data that are collected via system generated server logs, employees can ask their administrator to file a data subject access request via the DSR tool provided by Microsoft, and to provide a copy of the audit log pertaining to that employee.

According to Microsoft, the audit logs provide detailed information about product and service usage data contained in system-generated logs. The audit logs are created by Microsoft for security purposes, and provide a view for the user to access product and service usage data contained in the system-generated event logs. The

logs 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 the Connected Experiences, Exchange Online, SharePoint Online en OneDrive for Business

2. Personal data and data subjects

The Dutch government DPIA model requires that this paragraph 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. To help the individual data controllers, **Appendix 2** with this report contains a list of possible categories of personal data and data subjects.

The paragraph about personal data provides legal, technical and organisational arguments why the diagnostic data processed by Microsoft about the individual use of Office Online, the mobile Office apps, the Connected Experiences and the use of the cloud services SharePoint Online and OneDrive for Business are personal data.

This paragraph also provides a technical analysis of the telemetry data from the mobile Office apps, the results of a data subject access request for the diagnostic data about the use of Office Online and the outcomes of a Content Search for the diagnostic data relating to the use of the cloud storage and e-mail services.

2.1 Definitions different kinds of personal data

According to Article 4 (1) (a) 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.

In both DPIA reports about Office 365 ProPlus for SLM Rijk extensive legal, technical and organisational arguments are provided why the diagnostic data are personal data as defined in Art. 4(1) of the GDPR. Microsoft has since confirmed that the different diagnostic data may contain personal data. If diagnostic data are personal data, Microsoft has said it will include those data in the output of a Data Subject Request.[20]

The most recent DPIA report about Office 365 ProPlus from July 2019, describes Microsoft's ability to combine events over time because all diagnostic data are stored long-term in one database. Microsoft has admitted that Cosmos may contain end-user identifiable information (abbreviated by Microsoft as *EUII*) such as names and IP-addresses. These are stored in a hashed form. Microsoft also admits that Cosmos may contain logs with end-user pseudonymous identifiers such as User GUIDs, PUIDs, or SIDs (abbreviated by Microsoft as *EUPI*).

[20] Meeting report 28 August 2108, answer to Q2.

This last report also illustrates Microsofts ability to use the diagnostic data from its system generated server logs for analytical services. This will be elaborated in paragraph 2.5 of this report.

2.2 Diagnostic data mobile Office apps

At the moment, the collection of diagnostic data through the mobile Office apps is not transparent. Aside from the absence of a data viewer tool to inspect the telemetry data, Microsoft does not actively inform data subjects and administrators that it collects data about the individual use of the 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 for minimising 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.

Microsoft has announced, on its information page about the Office 365 ProPlus diagnostic data, that it will extend improved privacy controls to other Office clients in the coming months, such as Teams, Office for Mac, and the mobile apps, but it is not clear what these improvements will look like in practice.

Microsoft writes: "*We will be extending these new and improved privacy controls to additional Office clients, including Teams, Office for Mac, and our mobile 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.*"[21]

Privacy Company has performed three test runs with the same scenarios to intercept the diagnostic data that are sent to Microsoft from the in-built telemetry client in the mobile Office apps. During the first test run, Privacy Company has observed 37 different events in the iOS apps and 11 other events on Android, and only from Excel, not from the other Android apps. During the second test run, in total 88 different test runs have been observed, of which 77 on iOS and 17 (sometimes the same as on iOS) events on Android. See **Appendix 1** with this report. In order to repeat the findings with regard to the outgoing traffic to marketing company Braze, part of the scenarios were repeated on the iPhone X on 23 July 2019. This test has confirmed the previous findings.

It is technically not possible to completely document the captured data from the test devices. Since Microsoft has not published documentation with the specifications of the binary format in which the data are encoded, Privacy Company has made a *best effort* to distil the contents from the captured telemetry data.

This has resulted in partial data, where parts of non-textual data may be missing, and there is uncertainty about the beginnings and endings of individual events. Privacy Company has only looked at human readable data, not the binary data.

Based on experience with Office ProPlus and Windows telemetry, the consultants from Privacy Company know there are no empty fields. Therefore, every time a field name occurs in the decoded telemetry data, it is likely that this field has sent information, even if the captured example does not show binary, transformed data.

It is also plausible that all diagnostic events contain a header and content, similar to the events Microsoft collects via Windows and Office ProPlus. A typical diagnostic event contains a unique number, a few unique identifiers for the end user, his/her

[21] Microsoft Deploy Office, 6 May 2019, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/overview-privacy-controls

account and/or the administrator of the license (the *tenant*). These are typical header data. Next to the header data, the events contain content about the individual use of the different applications.

Microsoft provides the following description of events in Office 365 ProPlus:

> *"There is some information about events that is common to all events, regardless of category or data subtype. This common information, which is sometimes referred to as data contracts, is organized into categories. Each category contains fields, and these fields are the metadata and properties of an individual event. You can view this information by using the Diagnostic Data Viewer.*
>
> *The categories of information that is collected about events can be divided into two groups:*
>
> *Information common to all events*
> *Information that specifically supports diagnostic data collection"*[22]

All events from the mobile Office applications on the two different operating systems contain at least the two events DeviceInfo.id and Eventinfo.Time. That is, the unique identifier of the device and the exact time, up to 7 decimal places. The highlighted events in the four examples below show these unique identifiers and the ability for Microsoft to correlate different events from one user over time.

Example event PowerPoint version 10.64 on iOS (Microsoft.ApplicationInsights)


```
{
 "tags": {
 "ai.internal.sdkVersion": "iOS OneDrive: 1.0",
 "ai.session.id": "249ACE5C-2FFB-43F3-A558-629050CEAF1C",
 "ai.device.model": "iPhone (iPhone11,8)",
 "ai.user.id": "1003200044DDA640",
 "ai.device.osVersion": "iOS 12.2",
 "ai.session.isFirst": "true",
 "ai.application.ver": "10.64",
 "ai.user.accountId": "1003200044DDA640",
 "ai.device.network": "WF",
 "ai.device.language": "en-GB",
 "ai.device.id": "F8189EAF-313E-4199-97F6-9D1E861508F3"
 },
 "iKey": "AIF-155b372f-83bf-4a74-9474-cc4265f0e4f2",
 "name": "Microsoft.ApplicationInsights.aif155b372f83bf4a749474cc4265f0e4f2.Event",
 "time": "2019-05-09T14:49:04.399Z",
 "ver": 1,
 "data": {
 "baseData": {
  "properties": {
  "NetworkReachabilityStatus": "WiFi",
  "BuildType": "REAL_SHIP_BUILD",
  "ECSRampStates":
"{\"ramp_ios_uploadStepsTelemetryQos\":\"YES\",\"ramp_ios_explicitSessionInTelemetry\":\"
YES\",\"exp_ios_shareOnlyCommandBar\":\"YES\",\"ramp_ios_enableMAMCA\":\"YES\",\"ram
p_ios_3DWebEmbedPreview\":\"YES\",\"ramp_ios_floodgateSDK\":\"YES\",\"exp_ios_newExpe
```


[22] Microsoft, Required diagnostic data for Office, 10 June 2019, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/required-diagnostic-data

rimentSchemaValidationTernary2\":\"1\",\"ramp_ios_messageExtensionPixelationFix\":\"YES\"
,\"ramp_ios_multigeo_content\":\"YES\",\"exp_ios_premium_December2017UI\":\"0\",\"ramp
_ios_NotificationHandler\":\"YES\",\"ramp_ios_restoreOneDriveSetting\":\"YES\",\"exp_ios_loc
alKeychain\":\"YES\",\"ramp_ios_photosViewControllerPreload\":\"YES\",\"ramp_ios_lensSdkT
extStickers\":\"YES\",\"ramp_ios_massDeleteNotification\":\"YES\",\"exp_ios_ternaryDeviceEx
periment2\":\"1\",\"ramp_ios_qtContentResolverMetrics\":\"NO\",\"ramp_PowerLiftOnFeedbac
k\":\"YES\",\"ramp_ios_filterCrashAfterTermination\":\"NO\",\"ramp_ios_qtPolicyDoc\":\"YES\"
,\"ramp_ios_metadataCorruptionDetector\":\"YES\",\"ramp_ios_disablePdfAnnotationsWhileSy
ncing\":\"YES\",\"exp_ios_binaryDeviceExperiment2\":\"NO\",\"ramp_ios_semantic_zoom\":\"
YES\",\"ramp_ios_openInOfficeTelemetryFix\":\"YES\",\"ramp_ios_scanSiriShortcuts\":\"YES\"
,\"exp_ios_longFormFeatureCard\":\"0\",\"ramp_ios_lensSdkFilters\":\"YES\",\"ramp_ios_resp
ectIntuneAllowedAccounts\":\"YES\",\"ramp_ios_customenv1\":\"YES\",\"ramp_ios_expRemov
eDeletedItemsFromViewsKey\":\"runAsNeeded\",\"ramp_ios_ransomwareNotification\":\"YES\"
,\"ramp_ios_retryUpload\":\"YES\",\"ramp_ios_aaFlowValidationController\":\"YES\",\"ramp_io
s_braze\":\"YES\",\"ramp_ios_addCaptureAndRemoveMeTab\":\"YES\",\"ramp_ios_ackPushNo
tification\":\"YES\",\"ramp_ios_cameraRollNestedFolder\":\"YES\",\"config_ios_powerLiftTrigge
rsV2\":\"QoS\\/Authentication\\/SignIn?ResultType=UnexpectedFailure|Legacy\\/RefreshTaskI
nvalidData\",\"ramp_ios_useGenericManualUploadEventName\":\"YES\",\"ramp_ios_geomoveh
andling\":\"YES\",\"exp_ios_sharedWithMeUpdates2\":\"NO\",\"ramp_ios_premiumV1\":\"YES\
",\"ramp_ios_albumNotification\":\"YES\",\"ramp_ios_videoPlayerStreamingFallback\":\"YES\",
\"ramp_ios_accessTokenForHlsUrl\":\"YES\",\"ramp_ios_modifiedDateSort\":\"YES\",\"ramp_io
s_touchScrollerLabels\":\"YES\",\"ramp_ios_premiumSecurityMoment\":\"YES\",\"ramp_ios_m
oveHeicSettingToCameraBackup\":\"YES\",\"config_TimeoutMs\":\"300000\",\"ramp_ios_webE
mbedForCodeFiles\":\"YES\",\"exp_PremiumNavBarUpsell\":\"0\",\"ramp_ios_restoreCurrentTa
b\":\"YES\",\"ramp_ios_analyticsV2FetchVroomResourceIds\":\"NO\",\"ramp_ios_scanPromine
nceAnimation\":\"YES\",\"ramp_ios_sharedDiscoverAccessibility\":\"YES\",\"ramp_ios_writeWo
rkSiteData\":\"YES\",\"ramp_ios_qtContentResolverLongDelayIncidentMs\":\"5000\",\"ramp_io
s_lensSdkInk\":\"YES\",\"ramp_ios_onThisDayV2\":\"YES\",\"ramp_ios_networkSpeed\":\"YES
\",\"ramp_ios_renameDuplicateAutoUploadSession\":\"YES\",\"ramp_ios_analyticsV2Nov2018\
":\"YES\",\"ramp_ios_signOutAccountStorage\":\"YES\",\"config_Message\":\"custom
env1\",\"ramp_ios_semanticZoomFRE\":\"YES\",\"exp_ios_migrateSSOAppId\":\"YES\",\"ramp
_ios_recentSearches\":\"YES\",\"ramp_ios_gridViewTweaksApril2018\":\"YES\",\"ramp_ios_fas
tThumbnailProvider\":\"YES\",\"ramp_ios_siriShortcuts\":\"YES\",\"ramp_ios_gcodbshared\":\"
YES\",\"ramp_ios_cancelItemDespiteChunkUploadState\":\"YES\",\"config_ios_yellowFoldersS
urveySession\":\"10\",\"exp_ios_newExperimentSchemaValidationTernary\":\"1\",\"ramp_ios_
dontCheckChunkStateForCancellation\":\"YES\",\"ramp_ios_newExperimentSchemaValidationB
inary2\":\"NO\",\"ramp_ios_newExperimentSchemaValidationBinary\":\"NO\",\"ramp_ios_cam
eraBackupNewNameCheck\":\"YES\",\"ramp_ios_logCrossPlatQosEvents\":\"YES\",\"ramp_ios
_foregroundManualUploadSession\":\"YES\",\"ramp_ios_yellowCumulusFolders\":\"YES\",\"ra
mp_ios_newFileUploadMetrics\":\"YES\",\"ramp_ios_cameraUploadPermissionUpsells\":\"YES\"
,\"ramp_ios_discoverView\":\"YES\",\"ramp_ios_infiniteLoadingErrorBugFix\":\"YES\",\"ramp_i
os_offlineProgressToast\":\"YES\",\"exp_MicrosoftBrandedSISU\":\"2\",\"ramp_ios_createFlow
\":\"YES\",\"exp_ios_unknownSignInStateRecovery\":\"YES\",\"ramp_ios_lensSdkPhotoMode\"
:\"YES\",\"exp_ios_testNRT\":\"NO\",\"ramp_ios_odbAllPhotos\":\"YES\",\"ramp_ios_odbVroo
m\":\"YES\",\"ramp_ios_enableDbTransactionProfiler\":\"YES\",\"ramp_ios_bugFixDismissVC\"
:\"NO\",\"exp_ios_intuneManagedFilesExtension\":\"YES\",\"ramp_ios_retainSelectionOnCance
l\":\"YES\",\"ramp_ios_keepNameAlreadyInProgressErrorInFailedQueue\":\"YES\",\"ramp_ios_
yellowFoldersSurvey\":\"YES\",\"ramp_ios_ExpiringLinks\":\"NO\",\"ramp_ios_odbCameraBack
up\":\"YES\",\"ramp_ios_webEmbedForPpt\":\"YES\",\"ramp_ios_qtContentResolverMetricsThr
esholdMs\":\"2000\",\"ramp_ios_scanSaveAsReactNativePage\":\"YES\",\"ramp_ios_logSessio
nQosEventsV2\":\"YES\",\"ramp_ios_enableGetChangesMultiProcessSupport\":\"YES\",\"ramp
_ios_dragAndDropAlert\":\"YES\",\"ramp_ios_ignoreDuplicateUploadResponses\":\"YES\",\"ra
mp_ios_atp\":\"YES\",\"ramp_ios_quickFiltersIpad\":\"YES\",\"ramp_ios_nestedFoldersEducati
onBanner\":\"YES\",\"ramp_ios_quicklookPdfIos10\":\"YES\",\"exp_ios_ssoBackupKeychain\":\
"YES\",\"ramp_ios_vroom_sharedwithme\":\"YES\",\"ramp_ios_qtDataLayer\":\"YES\",\"ramp

_ios_vroomOdcGetChanges\":\"YES\",\"ramp_ios_whiteboardSharing\":\"YES\",\"ramp_ios_imageTranscoding\":\"YES\",\"ramp_ios_additionalSettingsTelemetry\":\"YES\",\"ramp_ios_photosUploadingSection\":\"YES\",\"ramp_ios_showFirstMonthFree\":\"YES\",\"ramp_ios_lensSdkTelemetry\":\"YES\",\"ramp_ios_lottieAnimationSupport\":\"NO\",\"ramp_ios_OnThisDayNotification\":\"YES\",\"ramp_ios_toastOverhaul\":\"YES\",\"ramp_ios_joinTestFlight\":\"YES\",\"ramp_ios_semantic_zoom2\":\"YES\",\"ramp_ios_newPhotosUI\":\"YES\",\"ramp_ios_customenv2\":\"YES\"}",
"TelemetryCorrelationId": "075FEDCF-0ABF-4289-A2E5-06469169834A"
},
"measurements": {},
"name": "ECS/RampValues",
"ver": 2
},
"baseType": "EventData"
},
"sampleRate": 100,
"seq": "249ACE5C-2FFB-43F3-A558-629050CEAF1C1017"
}

Example event Word on iOS (act_stats)

AppInfo.Language=en_GB-NL
tr_p=r_t
EventInfo.Sequence=1
DeviceInfo.OsBuild=Version 12.2 (Build 16E227)
n_ol_w=3
S_j=C++
n_inol=3
UserInfo.TimeZone=+02:00
S_k=ObjC
DeviceInfo.SDKUid=C9519B4-8ED8-476A-BC5B-2B534693535C
EventInfo.Time=2019-05-07T13:09:25.748Z
n_rcv_b=3855
DeviceInfo.OsName=iOS
rcv_b=3855
DeviceInfo.NetworkType=Wifi
DeviceInfo.Model=iPhone11,8
S_t=ACT
EventInfo.SdkVersion=ACT-iOS-ObjC-C++-8.4.3.0-ECS
records_received_count=3
TenantId=7d18e6b657034a70a865ff0a489df0a2
UserInfo.Language=en-NL
S_e=ECS
ol_w=3
inol=3
DeviceInfo.Id=8189EAF-313E-4199-97F6-9D1E861508F3
n_rcv_b_t=3855
rcv_b_t=3855
S_v=8.4.3.0
EventInfo.InitId=E97E898-67E3-4C27-AA1B-BFF8AAA964D2
eventpriority=4
EventInfo.Source=act_default_source
rcv_t=3
DeviceInfo.Make=Apple
AppInfo.Version=2.24

S_p=iOS
DeviceInfo.OsVersion=12.2
EventInfo.Name=act_stats
normal_priority_records_received_count=3

Example event Excel version 16.0.11601.20074 on Android (sqlite_policy_storage_load)

custom=sqlite_policy_storage_load
Event.CorrelationId=428ba265-a31c-4e6b-af3d-00007d8891c3
EventInfo.Source=act_default_source
DeviceInfo.Id=fc8d52a2660c998f
DeviceInfo.OsName=Android
AppInfo.Language=en-US
AppInfo.Version=16.0.11601.20074
UserInfo.Language=en-US
DeviceInfo.NetworkCost=Unknown
DeviceInfo.OsBuild=5148680
UserInfo.TimeZone=+02:00
EventInfo.InitId=3c9c0e90-ff1f-4b23-bab8-a3c85637debd
DeviceInfo.OsVersion=9
DeviceInfo.Make=Google
DeviceInfo.Model=Pixel 3
DeviceInfo.SDKUid=3b93d3f-dcd4-400c-87bf-807410d52e26
EventInfo.Sequence=21
Policy.EngineId=036fb6ba-9dc3-46e1-ab65-ab3a241a88f7_ADAL
EventInfo.Name=sqlite_policy_storage_load
EventInfo.SdkVersion=ACT-Android-Java-no-3.0.22.0-no
eventpriority=Normal
EventInfo.Time=2019-05-08T08:49:41.069Z
DeviceInfo.NetworkType=Wifi

Example event PowerPoint version 16.0.11601.20074 on Android (policy_sync_acquire_policy)

custom=policy_sync_acquire_policy
Event.CorrelationId=d50eaad3-998f-4805-9c1c-000092c7f584
EventInfo.Source=act_default_source
DeviceInfo.Id=fc8d52a2660c998f
DeviceInfo.OsName=Android
AppInfo.Language=en-US
AppInfo.Version=16.0.11601.20074
UserInfo.Language=en-US
DeviceInfo.NetworkCost=Unknown
DeviceInfo.OsBuild=5148680
UserInfo.TimeZone=+02:00
EventInfo.InitId=369cf29e-7583-4168-8477-871d10c739ff
Request.CorrelationId={F723D505-3DE4-4E1D-860F-00007CDF5F8B}
DeviceInfo.OsVersion=9
DeviceInfo.Make=Google
Request.Url=https://eur01b.dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies
DeviceInfo.Model=Pixel 3
DeviceInfo.SDKUid=bb6d6c17-cf8b-47a2-9f5b-6793a1fb8b4c
EventInfo.Sequence=13
EventInfo.Name=policy_sync_acquire_policy
EventInfo.SdkVersion=ACT-Android-Java-no-3.0.22.0-no

eventpriority=Normal
EventInfo.Time=2019-05-07T14:59:30.592Z
DeviceInfo.NetworkType=Wifi

The investigation of **the mobile Office apps for iOS and Android devices shows that Microsoft does not collect content data from files, e-mails or chats, nor file or pathnames.** In total, Privacy Company has observed 88 different kinds of telemetry events. Therefore, Microsoft collects far fewer diagnostic data through the mobile apps than through the installed versions of Office 365. Initially, Microsoft stated it collected between 23.000 to 25.000 different kinds of events about the use of Office ProPlus. It follows from the public documentation about the privacy improvements that have been implemented in the spring version of Office 365 ProPlus that this number has also been reduced substantially. In this documentation, Microsoft describes a little over 100 different telemetry events that register individual user actions. These events can each contain up to 100 fields, as well as 8 fields in the header.

Some events are sent very frequently. The app Teams on iOS for example has sent the event 'Scenario' 1.055 times to Microsoft, in the short time frame of the first test run. This event contains a large number of fields with information about the use of Teams, such as sending messages and collecting authentication tokens. The vast majority of the telemetry traffic is observed from iOS.

During the second test run, on 7 June 2019, no telemetry messages were sent from the PowerPoint and the Excel apps on iOS, while during the first test run quite a few telemetry messages were sent from the PowerPoint app. See **Appendix 1** with this report.

Outgoing traffic to US-based marketing company
The captured network traffic shows that some post requests are sent from the iOS apps Word, PowerPoint and Excel. The requests are sent to the domain mensa.iad.appboy.com.

This domain is currently owned by the US-based company Braze (www.braze.com) .

Braze writes it partners with Microsoft to directly offer its customer engagement services from Azure.[23] Braze writes in its Privacy Statement: "*Braze is a U.S. company, headquartered in New York, with global operations. Braze is a life-cycle engagement platform for companies around the world ("our Customers"), supporting stronger relationships between brands and their clients, primarily by leveraging first party data to personalize and automate lifecycle marketing campaigns through first party channels, such as email, mobile and web push notifications, and in-app/in-browser messaging. In practical terms, this means that we collect information for our use or on behalf of our Customers to customize messages to such visitors ("you"), including marketing messages, that you may find useful and to help Braze and our Customers understand your marketing preferences.*"[24]

Braze boasts on its website that it processes historical data and live data to create predictive data: "*We help leading brands create live views of their customers that stream and process historical, in-the-moment, and predictive data in an interactive*

[23] Press release Braze, Braze adds AccuWeather and Microsoft to Partner Ecosystem, 27 February 2018, URL: https://www.braze.com/blog/braze-partner-ecosystem/
[24] Braze Privacy Statement, March 2019, URL: https://www.braze.com/privacy/

feedback loop, so immediate action on insights can be taken with relevant messaging across mobile and web."[25]

Braze describes in its GDPR Compliance statement that it acts as data processor for its customers, that are the data controllers. Braze explains in this guidance that it has end user profiles based on the unique user and device identifier, and that controllers can access these profiles through either of these two identifiers:

"*The Braze Services can be configured to access an end user's User Identifier (defined by you) and/or device identifier. You may use either of these identifiers to export an end user Profile containing personal data from Braze's REST APIs, and to provide such personal data to a Data Subject in response to their request to access any personal data being processed by Braze as a Data Processor on your behalf."*[26]

Braze is not mentioned as sub-processor in the list of 77 companies provided by Microsoft that are sub-processors for the Online Services.[27]

In its Privacy Statement, Microsoft explains that it can share personal data with third parties, such as affiliates and vendors, but that those companies must abide by the Microsoft security and privacy requirements. Microsoft writes:

"*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."*

The fact that Microsoft requires such third parties to abide by Microsofts rules does not mean Microsoft has a GDPR-compliant data processor agreement with those parties.

Privacy Company has formally notified Microsoft of this observation on 18 June 2019, with a reminder sent on 3 July 2019. Microsoft has provided a brief reply to SLM Rijk on 19 July. Microsoft explains:

"*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."*[28]

Microsoft also notes that government organisations should give instructions to employees whether they may install other Microsoft consumer apps or apps from other providers on their (government issued) devices. Microsoft has not sent

[25] Braze homepage, URL: https://www.braze.com/.
[26] Braze, GDPR Compliance guide, URL: https://www.braze.com/docs/help/gdpr_compliance/#gdpr-and-your-braze-integration.
[27] Microsoft Personal Data Sub processors under the OST, 5 March 2019, URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2ouXb.
[28] E-mail Microsoft to SLM Rijk 19 July 2019.

additional information about the traffic to Braze in time for the publication of this report.

As described above, Privacy Company has specifically re-tested the findings with regard to Braze on 23 July 2019. These test confirm that the traffic to Braze is sent regardless of having logged in to a government Azure AD account with licensed use of the government Office 365 license.

In sum, the events from the mobile Office apps are personal data because every event contains a unique device identifier and timestamp. This information is, depending on the action the user performs, combined with information about the use of an application. This involves activities such as starting an app, retrieving data from SharePoint Online or OneDrive for Business, sending a message in Teams or Outlook, opening a calendar from Outlook, collecting authentication tokens from the Azure Active Directory, using file preview to view a file, or getting an error message.

Microsoft is able to identify an individual user based on the information in the different events Microsoft collects and stores for at least 90 days (see paragraph 10 of this report). As specialised technology company Microsoft must reasonably be able to combine events about individuals via the unique device identifiers and timestamps, and thus, directly or indirectly identify the data subjects.

2.3 Diagnostic data Office Online

At the moment, the data collection via Office Online is not transparent. Microsoft does not use its general information pages to inform data subjects and admins which diagnostic data it collects about the use of Office Online. Nor does Microsoft offer a choice for minimising 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.

Privacy Company has filed access requests in the name of an employee. Microsoft has been offering an automated solution for such requests since April 2018: The Data Subject Request (DSR) tool.[29] Microsoft uses this tool to provide system administrators with information about the use of the services in two ways: first, a set of data about the use of Office Online, and secondly, information about the use of the cloud storage and e-mail services.

In the results of the first type of Data Subject Request, about the use of the key applications in Office Online, Microsoft shows very little diagnostic data and no data at all about the use of the Connected Experiences. The results of the two data subject access requests only show that a directly identifiable person performed an action at a specific time (with 7 decimal places) in one of the five core applications, with which browser and from which operating system, but not what kind of action.

[29] Microsoft Blog, Nick Robinson, Introducing Data Privacy in Security & Compliance Center including Data Subject Requests experience, April 17, 2018, URL: https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Introducing-Data-Privacy-in-Security-amp-Compliance-Center/ba-p/183648 . See the extensive manual, Microsoft, Office 365 Data Subject Requests for the GDPR, URL: https://docs.microsoft.com/en-us/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.*"

Microsoft also registers whether there was a login error, what the cause was, and how the user was authenticated. The users are immediately identifiable in fields with the username and the e-mail address. The results of the access requests also contain the IP address used by the data subject, an indirect identifier.

Microsoft collects at least the following information about the use of the (browser based) Office Online applications: Date (UTC), Request Id, Correlation Id, UserID, User, Username, Application, Application ID , Resource ID, Resource, IP address, Location, Status, Sign-in error code, Failure reason, Additional details, Client App, Device ID, Browser, Operating System, Compliant, Managed, Join Type, MFA Auth Method, MFA Auth Detail and Conditional Access.

If the government organisations would only use Office Online without the connected cloud services, **Microsoft would not process any content from file, email, or chat content, nor any file or path names via this diagnostic data**. However, if the government organisations also use the cloud services, Microsoft does collect file and pathnames. This is explained in paragraphs 2.4 and 2.5 of this report.

The diagnostic data that Microsoft processes in its system-generated server logs about the use of Office Online are personal data, because the log files contain directly identifying data such as name, user name and e-mail address. Microsoft also acknowledges this, since it has provided access to these data as referred to in Article 15 of the GDPR. This shows that Microsoft is able to link the user's e-mail address to the user name, and to specific activities performed in the Online Office apps.[30]

2.4 Diagnostic data Connected Experiences

The captured traffic data does not contain any data about the use of the Connected Experiences in the mobile apps. Likewise, the results of the data subject access requests do not contain any data about the use of the Connected Experiences in Office Online.

This is remarkable, because Privacy Company made extensive use of different kinds of Connected Experiences in the test scenarios, insofar as these Experiences were available in the different applications in Office Online and as mobile apps. Privacy Company has used two Processor Connected Experiences (spelling checker and the translation module) and two Controller Connected Experiences (inserting a picture from the Internet and the LinkedIn CV assistant).

The data collection via the Connected Experiences is not transparent. Since May 2019, Microsoft has published information about the different types of Connected Experiences (for which Microsoft acts as processor or as a data controller). However, Microsoft does not provide any information about the types of personal data that it collects and processes via its cloud servers. Microsoft only writes that there are Connected Experiences that analyse content, but not how Microsoft handles these data.

Microsoft writes: "Connected experiences that analyze your content
Linked experiences that analyze your content are those that use your Office content to provide you with design recommendations, editing suggestions, insights into data and the like. Examples include PowerPoint Designer or Editor in Word.[31]

[30] Idem, p. 103.
[31] Microsoft, Connected experiences in Office, May 6, 2019, URL: https://docs.microsoft.com/nl-nl/deployoffice/privacy/connected-experiences.

Each of the services listed in the table below this explanation is clickable. The link to the Editor (the spelling checker) provides 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.*"[32]"

For an assessment of data subjects rights, see paragraph 15 of this report.

2.5 Diagnostic data cloud storage and e-mail services

Microsoft enables the administrators to access some of the individual diagnostic data it processes about the use of the cloud storage and e-mail services SharePoint Online, OneDrive for Business and Exchange Online. Administrators can access individual diagnostic data relating to the use of the cloud services through a Content Search in the Security & Compliance Center. This way, the administrators search the content that is still available on Microsoft's cloud servers as well as the system-generated log files from Microsoft's cloud servers.

Microsoft does not provide specific information about the data collection via these cloud storage and e-mail services.[33] Microsoft describes in its DSR manual what activities are recorded in audit logs, and that these logs are important to consult when a data subject files an access request.

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

[32] 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. This link provides more general information about spelling correction options in Word, URL: https://support.office.com/en-gb/Article/check-spelling-grammar-and-clarity-0f43bf32-ccde-40c5-b16a-c6a282c0d251

[33] Microsoft provides some public information about the Audit logs at: Search the audit log in the Security & Compliance Center, last updated 3 July 2019, URL: https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance and the subsection https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#audited-activities. Other information is available at Microsoft, Activity Reports in the Microsoft 365 admin center, 7 June 2019, URL: https://support.office.com/en-us/Article/activity-reports-in-the-office-365-admin-center-0d6dfb17-8582-4172-a9a9-aed798150263?ocmsassetID=0d6dfb17-8582-4172-a9a9-aed798150263&ui=en-US&rs=en-US&ad=US (all three sources last visited and recorded 8 July 2019). None of these sources provide a limitative overview of the types of personal data that Microsoft collects via system-generated event logs.

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."[34]

Microsoft recommends that admins create a separate query for each data subject access request.

"When you create a new case and start the search, these content locations are searched:
All mailboxes in your organization (including the mailboxes associated with all Microsoft Teams and Office 365 Groups)
All SharePoint Online sites and OneDrive for Business accounts in your organization
All Microsoft Teams sites and Office 365 group sites in your organization
All public folders in Exchange Online."[35]
The results of such a query contain 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.

These diagnostic data from the system-generated server logs about the use of SharePoint Online, OneDrive for Business and Exchange Online are evidently personal data, because they contain directly identifying data such as the user name, unique user ID as well as detailed data about activities performed on the cloud servers, as well as content data relating to the names of files and subject lines of e-mails.

Analytical services based on the system-generated log files
Microsoft uses the diagnostic data it collects through the use of the cloud storage and e-mail services to provide four kinds of analytical services. With MyAnalytics and Delve, Microsoft analyses data on individual work behaviour. Microsoft makes the insights available to every 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*".[36] Microsoft further explains: "*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*".

[34] 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
[35] Microsoft, Manage GDPR data subject requests with the DSR case tool in the Security & Compliance Center, 25 May 2018, URL: https://docs.microsoft.com/en-gb/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
[36] Microsoft, Office 365 Data Subject Requests for the GDPR, URL: https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365?toc=/microsoft-365/enterprise/toc.json

Through MyAnalytics, an employee not only gains insight into the amount of time he or she has spent on emails and meetings, but also, how many hours that individual 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*."[37]

Microsoft explains that the MyAnalytics service runs 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 organization'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*."[38]

About Delve, Microsoft writes: *"Delve uses intelligence to help employees discover relevant content and people across their organization. Users can only see documents they have access to."* Delve is based on the use of SharePoint Online and OneDrive for Business."[39]

The third analytical service offered by Microsoft is Workplace Analytics. This processing is based on the use of e-mail and the calendar, plus additional data that an employer can upload himself. According to Microsoft, Workplace Analytics only contains de-identified data: *Workplace Analytics contains aggregated, de-identified collaboration data of employees*. However, in an explanation of the system-generated log files, Microsoft clarifies that it considers de-identified data as pseudonymous data: "*Workplace Analytics also computes and stores pseudonymized data derived from Office 365 data to improve performance. If you would like to make this pseudonymized data available to a user and need assistance, contact Microsoft Support*."[40]

With Activity Reports in the Microsoft 365 admin center Microsoft provides administrators with detailed reports about all kinds of user activity per specific user, such as email activity, email apps usage, Skype, Yammer, Teams and OneDrive and SharePoint user activity.[41]

Based on the definition in Article 4(5) of the GDPR, pseudonymised data are personal data.

---

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

[38] Microsoft, MyAnalytics vs. Workplace Analytics, Delve, and the Microsoft Graph, URL: https://docs.microsoft.com/en-us/workplace-analytics/myanalytics/overview/privacy-guide#myanalytics-vs-workplace-analytics-delve-and-the-microsoft-graph. See also: 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.

[39] Microsoft, MyAnalytics vs. Workplace Analytics, Delve, and the Microsoft Graph, URL: https://docs.microsoft.com/en-us/workplace-analytics/myanalytics/overview/privacy-guide#myanalytics-vs-workplace-analytics-delve-and-the-microsoft-graph See also: 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 .

[40] Ibid.

[41] Microsoft, Activity Reports in the Microsoft 365 Admin Center, 7 June 2019, URL: https://docs.microsoft.com/en-gb/office365/admin/activity-reports/activity-reports?view=o365-worldwide

Microsoft warns admins that the Workplace Analytics may contain personal data. "*Insights in Workplace Analytics reports created by you may or may not contain personal data of users that your organization licensed for Workplace Analytics, depending on the information that your organization used to supplement the Office 365 data. Your Workplace Analytics administrator will need to review those reports to determine if they contain a user's personal data. If a report does contain a user's personal data, then you will need to decide if you want to provide a copy of that report to the user. Workplace Analytics allows you to export the report*."[42]
Employers are able to analyse individual work patterns on the basis of Workplace Analytics and thus make decisions about the productivity and commitment of an individual employee.

This is why the three analytical services that Microsoft has developed on the basis of the diagnostic data on the use of the cloud services linked to Office 365 are a good illustration that the diagnostic data that Microsoft processes via its own server-generated event logs are personal data.

2.6 Possible 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 Office diagnostic data. However, this report does provide some assistance to the *tenants* 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.

2.6.1 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. **Appendix 2** with this DPIA report contains an overview of possible categories of personal data and data subjects. Some kinds of data deserve extra attention.

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.[43]

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

[42] Microsoft, MyAnalytics vs. Workplace Analytics, Delve, and the Microsoft Graph.
[43] Amongst others, the categories of classified information are defined in the Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI).

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 the information stored on Microsofts cloud computers may include confidential information from and about government employees, including information which employees regularly access, send or receive labelled information. Such metadata may end up in system generated server logs.

Sensitive personal data

Some 'normal' personal data have to be processed with extra care, due to their sensitive character. 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, have a sensitive character. 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 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, analytic 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) GDRP, 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: special data may in principle *not* be processed. There are 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.[44]

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, in the snippets of content that may be captured, for example, information on crimes and convictions.

2.6.2 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. See **Appendix 2** with this report for more detailed suggestions for categories of data subjects.

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

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

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.

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 through diagnostic data

As summarised in the introduction and paragraph 2 of this DPIA, this DPIA assesses the risks of the processing of diagnostic data *about* the individual use of Microsoft Office Online and the mobile Office apps, in combination with the Connected Experiences and the usage data related to the use of SharePoint Online, OneDrive for Business and Exchange Online. As explained in paragraph 1.1 of this report, this DPIA distinguishes between three categories of data (content, diagnostic and functional data)

In this report, all data *about the individual use of the mobile Office apps, Office Online, the use of the 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 way the telemetry client captures data, is described in paragraph 8 of this report. The purposes for which Microsoft collects diagnostic data are described in the next paragraph of this report.

In the newly added explanation about the Connected Experiences, Microsoft also uses the term functional data, as one of three categories data collected by Microsoft:

- ***Customer content****, which is content you create using Office, such as text typed in a Word document, and is used in conjunction with the connected experience.*
- ***Functional data****, which includes information needed by a connected experience to perform its task, such as configuration information about the app.*
- ***Service diagnostic data****, which is the data necessary to keep the service secure, up to date, and performing as expected. Because this data is strictly related to the connected experience, it is separate from required or optional diagnostic data levels.*[45]

The diagnostic data provide Microsoft with quality information about the functioning of the applications. Those data reveal, for instance, when an application such as Word or PowerPoint is started by the user, how long it was opened, how the user worked in the application, and whether the system encountered any errors.

Microsoft gave the following fictive example of the contents of data that can be captured by the telemetry client on a device:

> "*A user types a word, hits the backspace button, types the word with a different spelling and repeats the cycle a few times. In such a case, we*

[45] Microsoft, Microsoft, Required service data for Office, 6 May 2019.

would like to use the telemetry data to learn that after a user uses backspace, we recommend to use the online dictionary."[46]

Microsoft gives the strongest privacy protections to Customer Data provided in Core Services (such as Office Online, SharePoint Online, OneDrive for Business, Skype for businesses and Teams). Microsoft has these data subjected to the more rigorous auditing of SOC-2, and covers the transfer of personal data from the EU to the USA with EU Standard Contractual Clauses (SCC).

Microsoft treats the personal data that are not Customer Data differently, depending on Microsofts own qualification of its role as a data controller, or as a data processor. As a data processor Microsoft protects the security of personal data outside of the scope of Customer Data following the requirements set forth in ISO 27001, ISO 27002, and ISO 27018.[47] As a data controller, Microsoft does not publish audit reports.

3.1 Anonymisation and pseudonymisation

Anonymisation is a complex and dynamic form of data processing.[48] Very often, organisations still possess original data in other databases, or continue to collect pseudonymised data.

As long as there is a realistic possibility to re-identify the masked data, the stored data cannot be considered anonymous and the organisation still needs a legal ground for the collection of the personal data and the purpose of anonymisation.

Even if the stored data are technically made irreversibly anonymous, (instead of hashed or encrypted), the rules of the GDPR apply from the start of the processing when the data are collected from an identifiable end-user and sent to Microsoft.

Microsoft has indicated that it deletes directly identifying data from the diagnostic data, and stores identifiers and URLs in a hashed format, instead of storing the original data. These are good technological measures to protect the confidentiality of the data. Since anonymisation strongly depends on the actual circumstances of the processing, any statement of anonymisation has to be verified technically.

As a result of the negotiations with SLM Rijk, Microsoft has added a contractual guarantee that it will follow the technical guidelines for (ongoing) anonymisation from the data protection authorities in the EU, as laid down in Opinion WP216. SLM Rijk has also obtained an effective possibility to audit compliance.

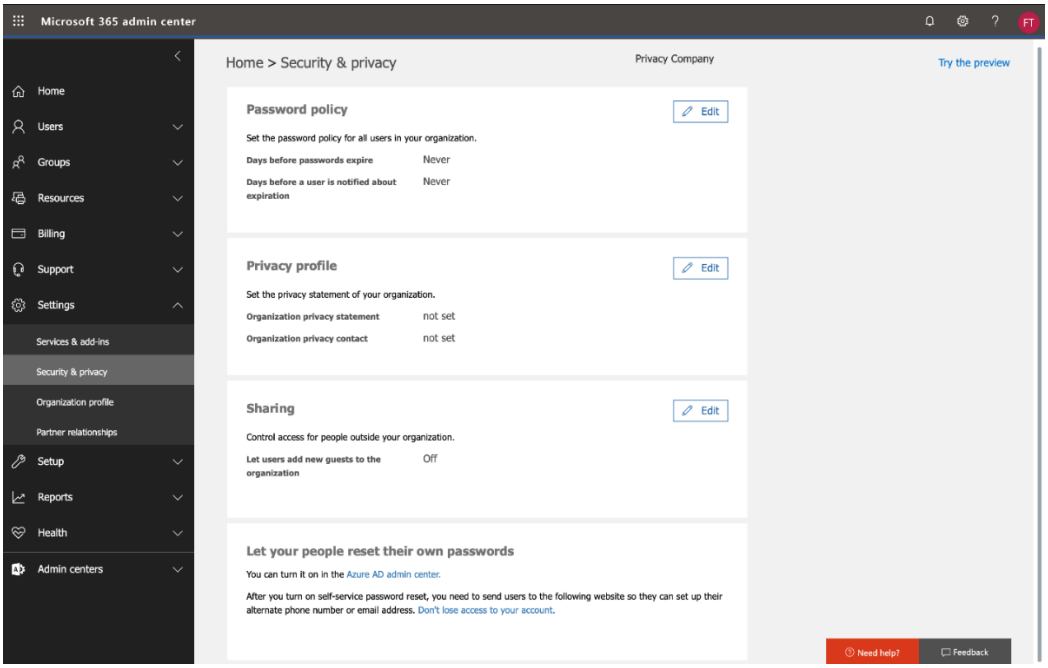
3.2 Privacy choices in Office Online and the mobile Office apps

With the introduction of the spring version of Office 365 Microsoft has announced some major privacy improvements for Office 365 ProPlus.[49] Amongst other, users can inspect the telemetry data with the existing Data Viewer Tool.[50] Administrators can choose a setting to minimise the telemetry data collection. Microsoft has also

[46] Meeting report 3 September 2018, new question renumber.
[47] Explanation provided by Microsoft in e-mail to SLM Rijk of 1 November 2018.
[48] See the Anonymisation Guidelines from the Article 29 Working Party, WP216, Opinion 05-2014 on Anonymisation Techniques, URL: http://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
[49] https://blogs.microsoft.com/on-the-issues/2019/04/30/increasing-transparency-and-customer-control-over-data/ See also: https://www.microsoft.com/en-us/microsoft-365/blog/2019/05/01/microsoft-office-new-privacy-controls/
[50] Microsoft, Using the Diagnostic Data Viewer with Office, https://support.office.com/en-us/Article/using-the-diagnostic-data-viewer-with-office-cf761ce9-d805-4c60-a339-4e07f3182855?ui=en-US&rs=en-US&ad=US

published extensive documentation about the contents of the telemetry events[51], and has changed its role for most of the Connected Experiences such as the spelling checker and the translation module to a role as data processor.[52]
There are no such choices with regard to the diagnostic data processing in Office Online. Microsoft does not offer options to administrators in the admin center under Security & Privacy to influence or minimise the diagnostic data flow.

Illustration 4: privacy settings for the admin of Office Online



Similarly, Microsoft does not offer any information or choices regarding the volume and nature of the telemetry data for the mobile Office apps to administrators. Inside of the apps, there are no privacy choices for users either.

Only if a user visits the separate settings for the different Office apps in the general menu in iOS, there is a possibility in three of the five apps to switch between basis and full levels of telemetry. No options are provided in Outlook and Teams. The settings screens for Word, Excel and PowerPoint are identical.

[51] Microsoft, Diagnostic data in Office, https://support.office.com/en-us/Article/diagnostic-data-in-office-f409137d-15d3-4803-a8ae-d26fcbfc91dd?ui=en-US&rs=en-001&ad=US
[52] Microsoft, Connected experiences in Office, URL: https://support.office.com/en-us/Article/connected-experiences-in-office-8d2c04f7-6428-4e6e-ac58-5828d4da5b7c?ui=en-US&rs=en-001&ad=US. Also see: Necessary service data (Connected experiences):, https://docs.microsoft.com/en-us/deployoffice/privacy/necessary-service-data/ Essential services events (Connected experiences), https://docs.microsoft.com/en-us/deployoffice/privacy/essential-services , List of services (Connected Experiences): https://docs.microsoft.com/en-us/deployoffice/privacy/connected-experiences Controller Connected Experiences: https://docs.microsoft.com/en-us/deployoffice/privacy/optional-connected-experiences

Illustration 5: settings in Word app on iOS

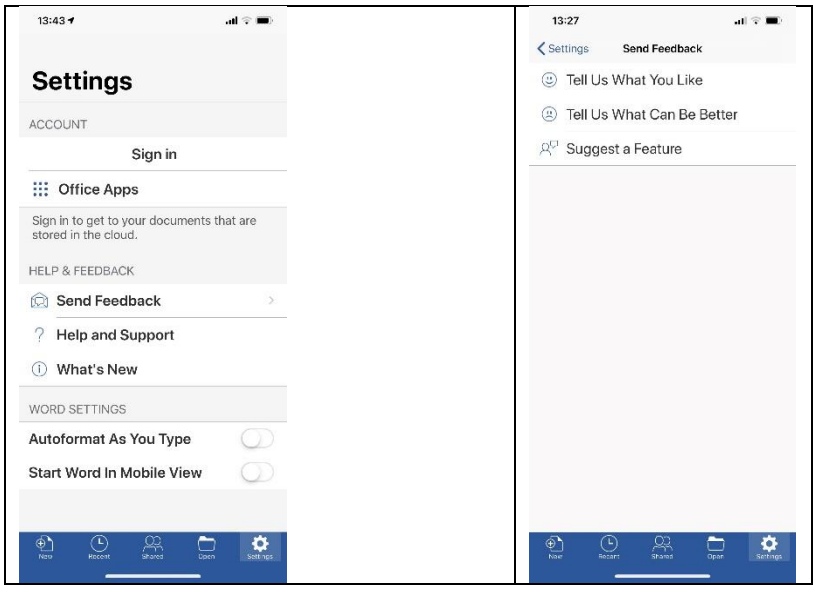
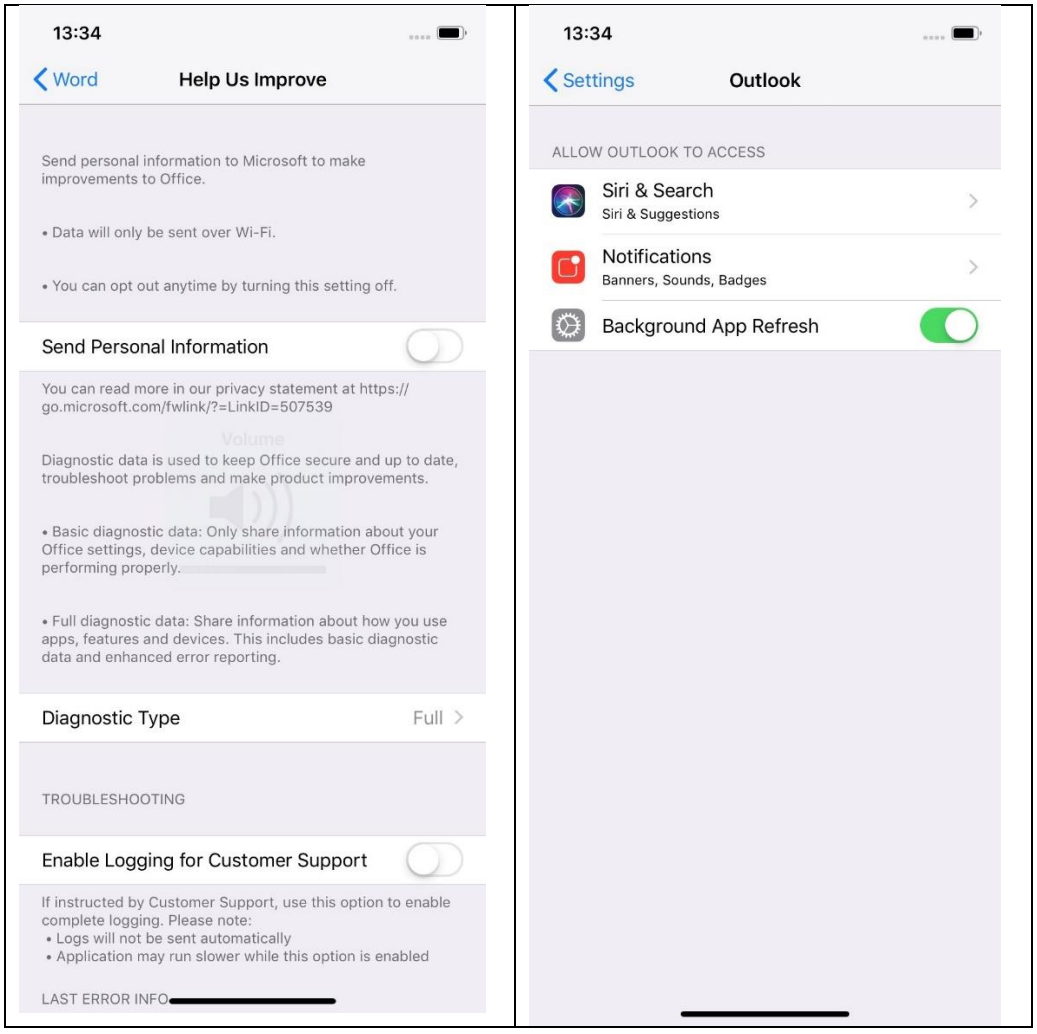


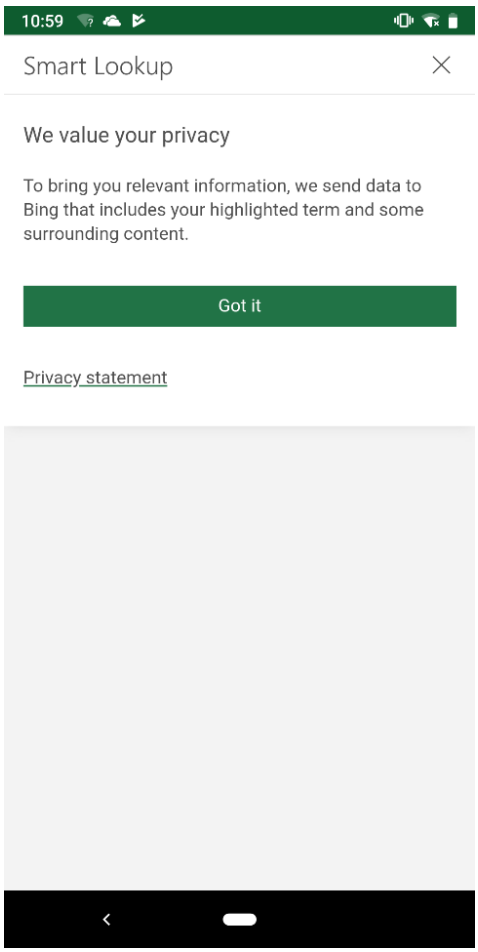
Illustration 6: choices in general OS settings Word app on iOS



Microsoft has announced privacy improvements for other Office clients, such as Teams, Office for Mac and the mobile apps, but it is not clear what these improvements will be, or when they will become available.

When an employee wants to use a Controller Connected Experience that relies for example on Bing or LinkedIn for the first time, Microsoft shows a warning that data will be sent to Microsoft. Microsoft writes in the pop-up that this doesn't just concern the marked search term, but also the surrounding information. Microsoft shows a hyperlink to its general Privacy Statement.

Illustration 7: warning first time use of Controller Connected Experience



Microsoft only shows this warning once in Office Online and in the mobile Office apps. If the user accepts, all Controller Connected Experiences are automatically turned on. The employee cannot see this, and cannot turn all Controller Connected Experiences off.

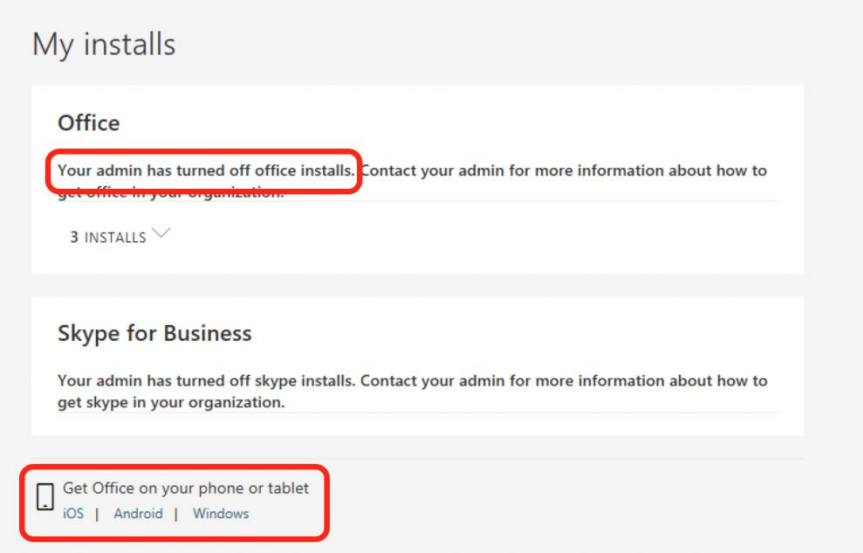
According to Microsofts public explanation these optional Connected Experiences are not part of the Office 365 license with government. Employees sign an individual contract with Microsoft for these services.

"*It is important to know that these optional cloud-backed services are not covered by your organization'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.*"[53]

Administrators do not have an option to prohibit users from downloading the mobile Office apps, unless they only work with fully managed devices. Employees can always go the iOS or Android appstore and download these apps.

[53] Microsoft, Deploy Office, Overview of optional connected experiences in Office, 6 May 2019, URL: https://docs.microsoft.com/en-gb/deployoffice/privacy/optional-connected-experiences

Illustration 8: No option for admins to prohibit downloads of mobile apps



4. Purposes of the processing

government organisations can use the diagnostic data about the use of the different services and applications offered in the Office 365 license to get information about access to personal data, to be able 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.

Microsoft processes the personal diagnostic data from Office Online and the cloud storage and mail services for different purposes than the diagnostic data from the mobile Office apps and the Controller Connected Experiences. This is a result of the fact that Microsoft considers itself to be a data processor for the online services and Office 365 ProPlus, but a data controller for installed software such as Windows 10 Enterprise and the mobile Office apps, and for the remaining 14 optional Controller Connected Experiences.

4.1 Results of negotiations purpose limitation with Microsoft

SLM Rijk has negotiated a number of additional contractual guarantees with Microsoft when it acts as a data processor. These results do not apply to services for which Microsoft is a data controller, such as the mobile Office apps and the Controller Connected Experiences.

The five most important results are:

1. Limitation to three purposes, where proportional
2. Guarantees apply to all kinds of personal data
3. Additional exclusions of profiling and data analytics
4. Amendment at the highest level of the enrolment framework
5. List of business operations for which Microsoft is a data controller
6.

1. Limitation to three purposes

As a data processor for Office 365 ProPlus and Office Online, the Connected Experiences and connected Cloud Services such as SharePoint Online, Microsoft acknowledges that it processes personal data through the metadata and will **only process these data 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.

2. Guarantees for all personal data
This strict purpose limitation applies to both the content (Customer Data) and to all diagnostic data, including the system-generated server logs.

3. Additional purpose exclusions
Microsoft has additionally **guaranteed that it won't use the content data or the diagnostic data from these data processor services for the purposes of profiling, data analytics, market research or advertising**, unless the customer explicitly requests Microsoft to do so. This includes a specific prohibition to use the personal data to show personalised recommendations on screen for Microsofts products and services that the customer has not purchased or does not use.

4. Amendment at the highest level
The contractual guarantees are created in the form of an amendment to the document that is the highest in the enrolment framework, the Microsoft Business and Services Agreement (MBSA). This ensures that no 'lower' ranking document can overrule the new limitations and guarantees.
Microsoft unilaterally imposes a number of conditions regarding compliance with European privacy regulations. The most comprehensive provisions are contained in the Online Service Terms (OST). These terms also include the EU model terms for transfers of personal data from a data controller in the EU to Microsoft in the United States.

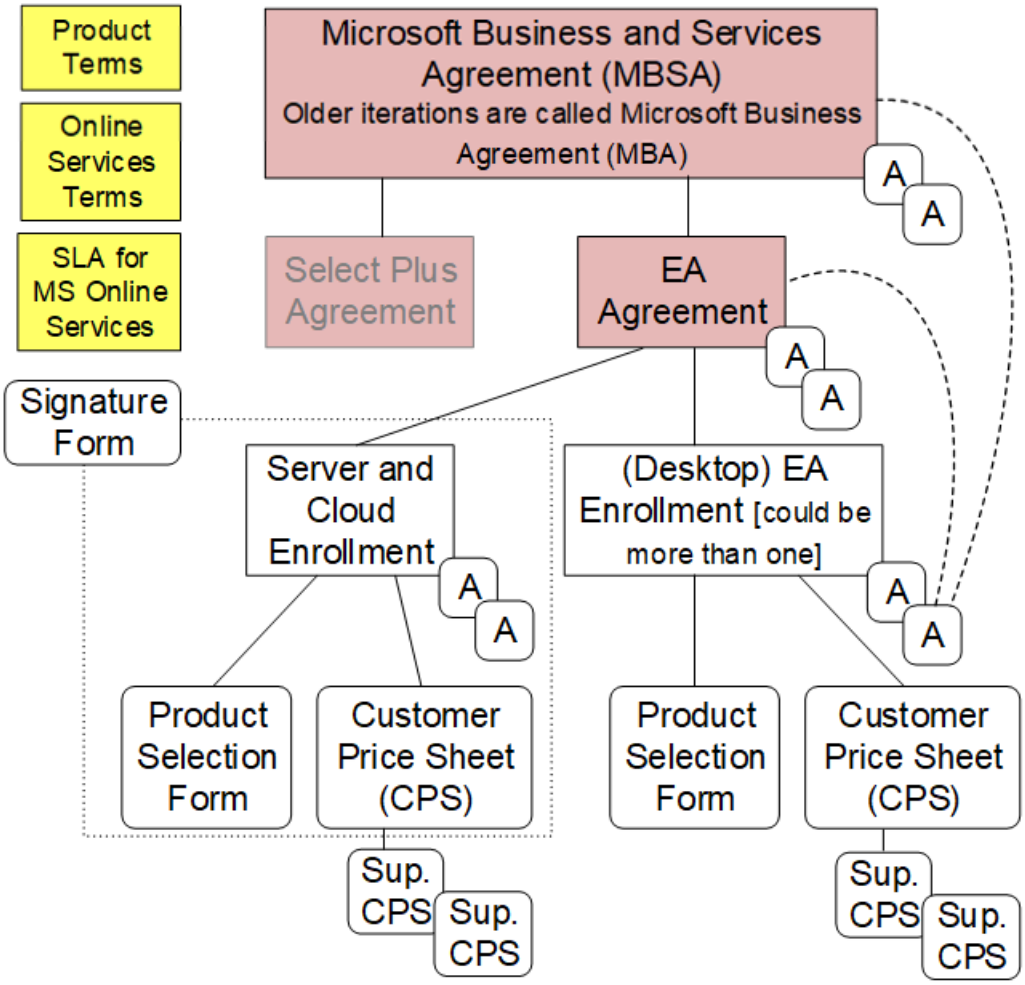
Normally, when a customer wishes to change the instructions for the processing, the changes to these instructions are applied in the same way as changes to the licensing agreement.[54]

As a hyperscale tech provider Microsoft does not conclude individual data processing agreements with individual Enterprise customers. Instead, the standard terms and conditions of Microsoft apply. As an annex to the OST, the pre-filled EU Standard Contractual Clauses (SCC) are included to legitimise transfer of personal data from the Netherlands to the USA.[55] Microsoft does not allow individual customers to determine the purposes in the SCC for which the personal data are processed. In the OST Microsoft states: "*Customer agrees that its volume licensing agreement (including the OST) along with Customer's use and configuration of features in the Online Services are Customer's complete and final documented instructions to Microsoft for the processing of Personal Data*."[56]

In the past SLM Rijk had already managed to negotiate a number of amendments on the standard agreement and standard terms. However, SLM Rijk did not have the ability to determine the purposes of the processing of diagnostic data, nor to specify which categories of personal could and could not be processed for each of these purposes, nor to individually consent to each sub-processor.

[54] OST May 2019, p. 8.
[55] Microsoft European Union model clauses backgrounder, January 2017, URL: https://aka.ms/eu-model-backgrounder (URL last visited and recorded on 8 July 2019).
[56] OST May 2019, p. 36, Annex 3.The clauses are between the government Enterprise tenant as data controller and 'exporter' and Microsoft Corporation in the USA as data processor and 'importer'.

Illustration 8: Contents of enrolment framework Office 365[57]



In the specific contract with the Dutch government, Microsoft repeated that the contract and use of features provide a complete list of instructions: "*The Enrolment (including these GDPR terms), along with Customer's use and configuration of features in the Online Services, are Customer's complete and final instructions to Microsoft for the processing of personal data.*"[58]

The new amendment overrules these previous amendments.

Following the Dutch government PIA model, the roles of Microsoft as data processor and as data controller will be described in more detail in paragraph 5 of this report, including the differences between Microsoft Ireland as the office signing the contract, and Microsoft Corporation as a data controller in the Privacy Statement.

5. List of business operations for which Microsoft is a data controller

Additionally, Microsoft has included a list of specific purposes of data processing related to business operations for which Microsoft is a data controller. These

[57] Graphic made by Directions on Microsoft, URL: https://www.directionsonmicrosoft.com/.
[58] Additional GDPR Terms included in Annex 1 to the GDPR Terms, Amendment ID M434, April 2017.

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 SLM Rijk, 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. In those circumstances, Microsoft acts as a data controller, to comply with legal obligations imposed under American law. This will be elaborated in paragraph 5.1 of this report (Microsoft as a data controller).

4.2 Purposes Office Online, Processor Connected Experiences and cloud storage and mail services

As a result of the negotiations with SLM Rijk, Microsoft only processes the diagnostic data about the use of Office Online, the processor Connected Experiences and the cloud storage and mail services for the three authorised purposes, and only where proportionate:

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

4.3 Purposes Controller Connected Experiences and mobile Office apps

With regard to the diagnostic data about the use of the 14 (optional) Controller Connected Experiences and the diagnostic data from the mobile Office apps, Microsoft considers itself to be a data controller, and processes diagnostic data about these services for all of the purposes mentioned in its Privacy Statement.[59]

Some of the purposes in the General Privacy Statement only apply to specific customer products and services, or have been specifically excluded in the OST, and are therefore not mentioned here.[60]

4.3.1 Purpose: compatible uses with providing the service

Microsoft outlines in its General Privacy Statement that it may use data for additional purposes it deems compatible.

"*General. When a customer tries, purchases, uses, or subscribes to Enterprise and Developer Products, or obtains support for or professional services with such products, Microsoft collects data to provide the service (including uses compatible with providing the service), provide the best experiences with our products, operate our business, and communicate with the customer.*"[61]

4.3.2 Purpose: Provide Our Products

The first specific purpose for the processing of all personal data, as mentioned by Microsoft, is to be able to provide the products in question.

"*We use data to operate our products and provide you rich, interactive experiences. For example, if you use OneDrive, we process the documents you upload to*

[59] Microsoft Privacy Statement, with monthly changes. The version used for this DPIA was last updated June 2019, available at https://privacy.microsoft.com/en-GB/privacystatement (URL last visited and recorded on 8 July 2019). In its confidential answer of 1 October 2018, answer 4C, Microsoft has confirmed that it processed the diagnostic data from the optional (Controller) Connected Experiences for all purposes in the Privacy Statement.

[60] These are the following purposes: Customer support, Promotional communications, Transacting commerce.

[61] Microsoft Privacy Statement, Product-specific details: Enterprise and developer products.

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."[62]

4.3.3 Purpose: Product improvement

The second purpose mentioned by Microsoft is improving its own products.

"*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 prioritise and voice data to improve speech recognition accuracy.*"[63]

4.3.4 Purpose: Personalisation

Microsoft processes personal data of users to personalise its services.

"*Many products include personalised 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 use Microsoft Account, with your permission, we can sync your settings on several devices. Many of our products provide controls to disable personalised features.*"[64]

4.3.5 Purpose: Product Activation

If any product offered by Microsoft needs to be activated, Microsoft also processes data in order to carry out this 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.*"[65]

4.3.6 Purpose: Product Development

Microsoft pursues the purpose of developing more products.

"*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.*"[66]

4.3.7 Purpose: Help secure and troubleshoot

Microsoft processes data in order to secure and troubleshoot its products.

"*We use data to help secure and troubleshoot our products. This includes using data to protect the security and safety of our products and users, 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.*"[67]

[62] Microsoft Privacy Statement, How We Use Personal Data.
[63] Ibid.
[64] Ibid.
[65] Ibid.
[66] Ibid.
[67] Ibid.

4.3.8 Purpose: Safety

Microsoft processes personal data in order to protect the safety of products.

"*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.*"[68]

4.3.9 Purpose: Updates

Microsoft processes personal data in order to roll out 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 maximise your experience with our products, help you protect the privacy and security of your data, provide new features and ensure that your device is ready to process such updates.*"[69]

4.3.10 Purpose: Relevant Offers

Microsoft wants to use all kinds of data to send relevant offers.

"Microsoft uses data to provide you with relevant and valuable information regarding our products. ***We analyse 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.*"[70]

4.3.11 Purpose: Advertising

"*Microsoft does not use what you say in email, chat, video calls or voicemail, 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.*"[71]

Microsoft mentions the sharing of personal data with third parties for advertising purposes. Microsoft does not publish an overview of these third parties, and only provides examples of obvious advertising networks. Microsoft does specifically mention the use of usage data from Microsoft products and sites for advertising purposes. Microsoft omits to explain that this also involves the usage of the mobile Office apps and the Controller Connected Experiences.

"*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, as well as the sites and apps of our advertisers and partners.*** *We refer to these ads as "interest-based advertising" in this statement.*"[72]

[68] Ibid.
[69] Ibid.
[70] Ibid.
[71] Ibid.
[72] Ibid.

4.3.12 *Purpose: Reporting and Business Operations.*
Microsoft collects and processes information for reporting and business operations:
"*We use data to analyse our operations and perform business intelligence. This enables us to make informed decisions and report on the performance of our business.*"[73]

4.3.13 *Purpose: Protecting rights and property.*
Microsoft analyses personal data of users in order to protect her (intellectual property) rights.
"*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 licences 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.*"[74]

4.3.14 *Purpose: Research.*
Microsoft explains that it does research with the data:
"*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.*"[75]

5. Controller, processor and sub-processors

The different roles of the involved (commercial) parties in the processing of personal data are defined in Article 4(7) to (4) 9 GDPR.

'controller' means 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;
'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Article 26 of the GDPR specifies the obligations for joint controllers to create a transparent agreement about their roles and responsibilities.

Article 28 of the GDPR specifies the obligations of data controllers versus data processors. Article 28(3) lays down eight specific obligations of the data processor, such as only processing the personal data on documented instructions from the controller, and for example contribute to audits. Article 28(4) describes the possibility for a processor to engage another processor to carry out specific processing activities on behalf of the controller. These are sub-processors.

Based on the OST that are part of the contractual framework between SLM Rijk and Microsoft, Microsoft qualifies itself as a data processor for the processing of the content data it collects through the use of Connected Experiences, and the use of cloud storage and mail services SharePoint Online, OneDrive for Business and Exchange Online. This role as data processor also applies to personal data Microsoft collects about the use of Office Online. However, a formal legal assurance that a service provider acts as data processor, is not enough. The roles of data controller

[73] Ibid.
[74] Ibid.
[75] Ibid.

and data processor have to be determined based on a factual and formal analysis of the case, taking all relevant circumstances into account.

With regard to the processing of diagnostic data about the usage of Office Online and the mobile Office apps, there are three possible scenarios for the processing of Office functional data by Microsoft.

1. Microsoft as a data processor, the individual government organisation as a data controller
2. Microsoft as a data controller, the individual government organisation as joint data controller
3. Microsoft as a data controller, in a direct relation with the natural person who is the end-user of the software

5.1 Results of negotiations Microsoft as data processor

As a result of the negotiations with SLM Rijk, since the release of version 1904 of Office 365 ProPlus on 29 April 2019, Microsoft provides comprehensive documentation what kind of personal data Microsoft processes about the individual usage of the Office ProPlus software and has upgraded the data viewer tool to decode the diagnostic data from Office as well as those from Windows.

Microsoft has also reorganised its Connected Experiences. Microsoft now offers many frequently used services such as the Spelling Checker and the Translator as a data processor. If they have upgraded to the most recent version of Office 365 ProPlus, administrators can centrally block the use of the Controller Connected Experiences, and some or all of the Processor Connected Experiences. However, these controls are not available in Office Online and the mobile Office apps.

These technical and organisational mitigating measures apply worldwide, to all Office 365 users. In the specific contract with SLM Rijk, Microsoft has taken additional legal measures to guarantee that all personal data, regardless of their classification as Customer Data or as diagnostic data, will only be processed for three authorised purposes, where proportionate, and no data will be used for any kind of data analytics, profiling, marketing research or advertising.

Because the purposes have contractually been limited to the three purposes that are necessary to deliver an up-to-date and secure service, Microsoft can now qualify as a data processor for the processing of metadata about the use of Office 365 ProPlus, Office Online, the Connected Experiences and connected Cloud Services such as SharePoint Online.

As a data processor, Microsoft no longer determines itself what purposes are compatible with the main purpose of providing the service. The additional exclusions of 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’.

These legal guarantees allow the Dutch government organisations to fulfil their role as data controllers for the diagnostic data from Office 365 ProPlus, the cloud storage and mail services and Office Online. However, these contractual guarantees do not apply to the processing of diagnostic data from the Controller Connected Experiences and the mobile Office apps.

Effective audit rights

Additionally SLM Rijk has successfully negotiated the ability to organise an annual audit, to be performed by an independent auditor, also with regard to sub-processors, to verify compliance with the agreed data processing. SLM Rijk has the ability to organise further audits in case of incidents, relating to the context of the incident.

The audits organised by Microsoft itself relating to personal data outside Customer Data are ISO audits. They only examine the structure of rules and the existence of checks, but not how the data are factually processed.

The right to audit is an important element of the EU Standard Contractual Clauses.[76] This right enables the data controller (the Enterprise customer) to verify whether the actual data processing is in accordance with the high level of data protection granted in the EU. Although formally the right to audit was not removed from the pre-filled EU Standard Contractual Clauses, Microsoft did not offer a reasonable possibility for verification by an independent auditor hired by the Dutch government or to add extra audit questions to audits organised by Microsoft.
The right to audit from the SCC only applies to data processor services, not to the services Microsoft provides as a data controller.

Control over sub-processors
SLM Rijk has also successfully exercised its right to inspect some contracts with sub-processors, as guaranteed in the Standard Contractual Clauses. Microsoft previously did not give copies of its contracts with sub-processors, but was willing, on request, to provide a copy of addenda on the standard contractual clauses.[77] Microsoft is now committed to work on further transparency, to prevent that government institutions would have to give blanket consent to all sub-processors used by Microsoft.

Microsoft provides a reference to a list of sub-processors in its terms and conditions. Currently, the list has 77 companies.[78] Microsoft has given the reassurance that Microsoft itself governs the access from all sub-processors to Customer Data, including personal data.

Microsoft writes: "*The sub-processors have to authenticate with us. Sub-processing is always done inside of (or plugged into) Microsoft-systems, and therefore we regulate their access to the data the same as within our internal organisation. Microsoft can provide adequate evidence of compliance even when processing has been done by sub-contractors. If you have an evidence request, we can provide the evidence to the same standard as our own service. When our auditor Deloitte audits our system, there is no need for them to visit specific sub-processors, since the sub-processors cannot do anything outside of Microsoft's systems.*"[79]

[76] Clause 5(f) of the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU). *The data importer agrees and warrants: (…) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;"* Microsoft states in its response to the initial Office 365 ProPlus DPIA that the DPAs have confirmed that this approach is consistent with the EU Model Clauses, including clause 5(f) thereof. No source is provided of this validation.
[77] Meeting report 30 August 2018, answer to Q41.
[78] Microsoft overview OST sub-processors, 5 March 2019, URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2ouXb
[79] Meeting report 30 August 2018, answer to Q40.

The right to inspect contracts with sub-processors from the SCC only applies to data processor services, not to the services Microsoft provides as a data controller.

Retention periods
As will be described in paragraph 10 of this DPIA, Microsoft (still) determines the retention periods for the diagnostic data, rather than the Enterprise customers. 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.*"[80]

Determining how long data can be stored, is a decision that can only be taken by a data controller. Deciding how long data are available, is a decision about the means of the processing. Microsoft has published more information about the different kinds of active and passive deletion of data, but does not yet provide means for organisations to delete historical diagnostic data. The data protection risk of this processing is assessed in paragraph 16.2.7 of this report.

5.2 Microsoft as data controller with regard to legal orders

As described in paragraph 4.1 of this report, when Microsoft has to process some personal data from its customers for its own legitimate business purposes, it acts as a data controller. This is the case when Microsoft has to hand over personal data from customers to law enforcement authorities or security agencies / secret services.

There is also a risk that law enforcement sends a subpoena to a sub-processor after Microsoft has refused the request. In such cases, the subcontractor may be legally forced to hand over data without involvement of Microsoft or of the tenants. However, such access is only possible within the compliance boundaries determined by Microsoft. According to Microsoft, subcontractors cannot physically comply if they don't have the keys.[81]

Microsoft publishes a bi-annual transparency report. In the Netherlands, in the period July-December 2018, Microsoft received 176 law enforcement requests, relating to 222 accounts/users.[82] Microsoft explains that very few law enforcement requests relate to Enterprise cloud customers.[83] Microsoft states there is a very high legal bar for blind requests in the Enterprise environment (where Microsoft would get a nondisclosure order). The requesting authority would have to prove that the board of the government organisation cannot be trusted.

[80] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q8 (preamble).
[81] Meeting report 30 August 2018, answer to Q40 and Q41.
[82] Microsoft Law Enforcement Requests Report, URL: https://www.microsoft.com/en-us/about/corporate-responsibility/lerr (URL last visited and recorded on 8 July 2019).
[83] Ibid. *In the second half of 2017, Microsoft received 47 requests from law enforcement for accounts associated with enterprise cloud customers. In 16 cases, these requests were rejected, withdrawn, or law enforcement was successfully redirected to the customer. In 24 cases, Microsoft was compelled to provide responsive information: 12 of these cases required the disclosure of some customer content and in 12 of the cases we were compelled to disclose no content information only. Three of the requests are still pending resolution*.

Although Microsoft also publishes bi-annual reports about orders from the security agencies, through FISA-orders, these reports only provide total aggregate estimates, not split per country or per type of customer (consumer or Enterprise).[84]

Microsoft mentions the possibility of legally mandatory disclosure of data to law enforcement as a data processor in the Online Service Terms. According to the relevant provision, Microsoft "*will not disclose Customer Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) as described in the OST, or (3) as required by law.*"[85]

When law enforcement compels Microsoft to disclose Customer Data, Microsoft commits to trying to redirect the request to the customer (the data controller), and only disclose data directly to law enforcement agencies when compelled to do so. In these cases, Microsoft commits to notifying the customer promptly of the access.[86]

Microsoft writes: "*Microsoft will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.*"[87]

This promise does not apply to the diagnostic data from the mobile Office apps and the Controller Connected Experiences, because the OST do not apply. In its general Privacy Statement Microsoft only states it will disclose personal data, including content "*when we have a good faith belief that doing so is necessary to do (…) Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies.*"[88]

When Microsoft is obliged itself to hand over personal data to law enforcement and security agencies / secret services, for example under the USA CLOUD Act and under FISA orders, Microsoft acts as a data controller, not as as data processor. When the order involves an obligation to comply with foreign legal obligations, to countries without an adequate level of data protection and without an international treaty, this does not provide a valid legal exception for data controllers in the EU to transfer personal data. The legal complications of transfer of personal data from the EU to the USA will be elaborated in paragraph 7 of this report.

In sum, the Dutch government organisations clearly cannot instruct Microsoft to process data in violation of the GDPR, when Microsoft has to comply with US American legal orders. As will be assessed in paragraph 16.2.8 this legal paradox can only be solved by legal measures at the EU level.

5.3 Microsoft as data controller for the optional Connected Experiences and the mobile Office apps

Microsoft considers itself to be an (independent) data controller for the diagnostic data it collects via the use of the 14 optional (Controller) Connected Experiences, and for the data processing via the mobile Office apps. Microsoft itself has

[84] Microsoft, U.S. National Security Orders Report, URL: https://www.microsoft.com/en-us/corporate-responsibility/fisa. For example, in the first half of 2018, Microsoft received between 0 – 499 orders for content, relating to 13,000 - 13,499 accounts.
[85] OST May 2019, p. 7.
[86] Ibid.
[87] Ibid.
[88] Microsoft general Privacy Statement, last updated June 2019.

determined the purposes of the processing (all 14 purposes of the Privacy Statement), including transfer of diagnostic data from at least three of the mobile Office apps for iOS to an US American-based marketing company. Microsoft processes the diagnostic data from the Controller Connected Experiences and the mobile Office apps based on the consent of the end-user, the government employee.

Different from the new controls build by Microsoft in Office 365 ProPlus, government administrators cannot technically prohibit the use of the Controller Connected Experiences via Office Online and via the mobile Office apps. They are also unable to prevent users from downloading the Office apps via the Microsoft Store, and connect with their work account.

SLM Rijk has worked with Microsoft to improve transparency and logic for end-users, by ensuring that Microsoft would only act as a data processor for the most widely used and practically indispensable functionalities such as the spelling checker (Editor) and the Translator module.

Data processing related to usage of productivity tools at work should not be based on consent of the employees. SLM Rijk would have preferred if the data processing related to all the Connected Experiences were to take place within the clear processor boundaries. Microsoft has explained why it is not willing to do so: because these data are used for the commercial activities from its search engine Bing and social network LinkedIn. Microsoft considers the mobile Office apps to be consumer software, accessible for anybody worldwide via the Apple Appstore and Google Play, like all other apps users can install on their mobile devices.

Notwithstanding Microsofts position, Microsoft is not the only data controller responsible for this diagnostic data processing. Because Dutch government organisations that make their employees work with Office 365 allow Microsoft to process these data, they are joint controllers with Microsoft for the processing of diagnostic data from the mobile Office apps and the Controller Connected Experiences.

5.4 Microsoft and government organisations as joint controllers

The conclusion of the first Office 365 ProPlus DPIA report for SLM Rijk was that the government organisations and Microsoft were joint controllers for the processing of the diagnostic personal data about the use of the different Office 365 applications and services. This analysis was based on jurisprudence of the European Court of Justice. The EUCJ has clarified in two recent rulings[89] and an advice from the Advocate General[90] that parties may very soon be held to be joint controllers, even if they do not have access to all the data collected by the other party, and also when the levels of responsibility are very unevenly divided. While both rulings originate in disputes about the European Data Protection Directive, the definition of joint controller did not materially change in the GDPR. The GDPR only adds extra obligations (in Article 26) for joint controllers to transparently determine their roles and responsibilities.

[89] European Court of Justice, C-210/16, 5 June 2018, Abhenries Landeszentrum für Datenschutz Schleswig-Holstein versus Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388. See in particular par. 38-43. See also: Case C-25/17, 10 July 2018, Tietosuojavaltuutettu versus Jehovah's Witnesses — Religious Community, ECLI:EU:C:2018:551, par. 66-69.

[90] European Court of Justice, C-40/17, advice Advocate General Bobek, 19 December 2018, ECLI:EU:C:2018:1039.

Because government organisations are unable to technically prevent their employees from using the Controller Connected Experiences and the mobile Office apps, and thus allow Microsoft to process the personal data for its own purposes, they are joint controllers with Microsoft for the processing of personal data about the use of these services. This includes the transfer of diagnostic data to the US-based marketing company Braze.

5.5 Roles of Microsoft Corporation and Microsoft Ireland

The Dutch government organisations sign a contract with Microsoft Ireland, but the data processor for most of the Office diagnostic data is Microsoft Corporation in the USA. Both the Online Service Terms and the GDPR clauses, including the EU Model Clauses, refer to, and are signed by, Microsoft Corporation. The USA mother organisation is also the data controller with regard to the optional (Controller) Connected Experiences, since Corporation determines the global purposes and means for the processing.[91] Additionally, all Office telemetry data are sent to a single end-point in the USA, where engineers from Microsoft Corporation may use the diagnostic data for analysis purposes.

6. Interests in the data processing

This paragraph 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 paragraph 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. The authorisations of the network drives are generally more difficult to organise and to manage. This entails the privacy and security risks of users having access to documentation to which they should not have access based on their role. 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 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 administration 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, and the use of Office Online and the mobile Office apps allows the government to cut back spending on work spaces in offices. Because Microsoft

[91] The Dutch DPA provides a detailed explanation of the roles of Microsoft Corporation, Microsoft Ireland and Microsoft Netherlands B.V. in its Windows 10 telemetry investigation report. See paragraph 2.2 of this report. In sum, Microsoft Ireland is a relevant establishment of Microsoft Corporation, but the role of establishment should not be confused with the role of data controller. See pages 105-112 of the Dutch DPA report.

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 possible 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 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.[92] Microsoft explains: "*Our users don't simply use a workstation at a desk to do their jobs anymore. They're using their phone, their tablet, their laptop, and their desktop computer, if they have one. It's evolved into a devices ecosystem rather than a single productivity device (…).*"[93]

Microsoft has explained 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.*"[94]

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 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

[92] 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/.
[93] Idem.
[94] Meeting report 30 August 2018, answer to Q46.

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."*[95]

Nonetheless, as a result of the negotiations with SLM 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".[96] 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.[97] Microsoft writes about this in its 2018 annual report: "*Our Search business, 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***."[98]

Microsoft does not offer a sovereign country cloud to countries, with the exception of the cloud for China, the German cloud, 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.[99] 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.[100]

6.3 Joint interests

[95] Meeting report 29 August 2018, answer to Q16.
[96] Meeting report 29 August 2018, answer to. Q30.
[97] 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-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.
[98] Idem, p. 10.
[99] Meeting report 29 August 2018, answer to Q21.
[100] Meeting report 29 August 2018, answer to Q21.

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.[101] 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.

7. Transfer of personal data outside of the EU

The GDPR contains special requirements for the processing of personal data outside of the European Union. A controller may process data in a country with an adequate level of protection of personal data, as decided by the European Commission. That means that the level of data protection in that country is comparable to the level of protection in the European Economic Area (the EU member states and Iceland, Liechtenstein and Norway).

There is a special arrangement between the United States and the European Union about the protection of personal data. The Privacy Shield (previously Safe Harbour) allows US American undertakings to 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.

It is also possible to transfer personal data from the EU to a third country using Standard Contractual Clauses, as drafted by the European Commission under the Data Protection Directive. These clauses aim to contractually ensure a high level of protection. Microsoft uses a combination of two measures: Privacy Shield and the EU Standard Contractual Clauses (SSC).

The SCC apply to the Online Services such as Office Online and the processor-based Connected Experiences, and as a result of the negotiations with SLM Rijk, also to Office 365 ProPlus. Personal diagnostic data from the Controller Connected Experiences and the mobile Office apps, however, are transferred under the terms of the EU-US Privacy Shield Framework. Microsoft has self-certified under this regime.[102] Although both of these transfer mechanisms are legally valid, and approved by the European Commission, there is serious doubt about the future validity of these instruments with regard to transfers to the USA. Both instruments are subject of a procedure at the European Court of Justice. The Court is asked to decide whether this type of agreement is sufficient mitigation for the risks of extensive surveillance in the USA as brought to light by whistle blower Edward Snowden, also with regard to the interception of data in transit.[103]

[101] To the extent legally allowed without separate consent by the ePrivacy Directive and future ePrivacy Regulation. Roughly summarised, 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.
[102] Microsoft is an active participant in the Privacy Shield Framework https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK&status=Active.
[103] 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. The court hearing took place on 9 July 2019. Advocate General Henrik Saugmandsgaard Øe will publish his Opinion on 12 December 2019. IAPP, CJEU's hearing on Schrems II has both sides worried ruling could be sweeping, 9 July 2019, URL: https://iapp.org/news/a/cjeus-hearing-on-schrems-ii-has-both-sides-worried-ruling-could-be-sweeping/. For Dutch speaking people, the ministry of Foreign Affairs publishes an overview of the different steps in this procedure at

In its OST[104], Microsoft guarantees that a limited sub category of data from Core Services which Microsoft defines as Customer Data, will only be stored in EU data centres.
"*If Customer provisions its tenant in Australia, Canada, the European Union, France, India, Japan, South Korea, the United Kingdom, or the United States, Microsoft will store the following Customer Data at rest only within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, (3) files uploaded to OneDrive for Business, and (4) project content uploaded to Project Online.*"[105]

Microsoft details the different data centres it uses for the different Office 365 services. The actual storage of *data at rest* in the different data centers varies per service. This is for example different for Outlook and for SharePoint Customer Data. In case of SharePoint Online and OneDrive for Business, the data are stored in data centres in the Netherlands and in Ireland.[106]

Microsoft can be ordered to provide access to the data to US authorities to data stored in data centres in the EU. The USA CLOUD Act essentially extends jurisdiction of the US American courts to all data held by American corporations, even when that data is stored in data centres outside of the territory of the United States.

As analysed by the European Data Protection Board and the EDPS in their recent advice to the LIBE Committee of the European Parliament about the CLOUD Act, transfers of personal data from the EU have to comply with Articles 6 (legal grounds) and 49 (exceptions to allow for transfer). In case of an order based on the US CLOUD Act, the transfer can only be valid if recognised by an international agreement between the EU and the USA.

"*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).*"[107]

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.*[108] Additionally, the data protection authorities

---

https://ecer.minbuza.nl/ecer/hof-van-justitie/nieuwe-hofzaken-inclusief-verwijzingsuitspraak/2018/c-zaaknummers/c-311-18-facebook-ireland.html. 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 to allow the court to first deal with the Schrems-2 case.

[104] Microsoft Online Service Terms Microsoft, May 2019.

[105] Idem, p. 10.

[106] Microsoft, Where is your data located, URL: https://products.office.com/nl-NL/where-is-your-data-located?ms.officeurl=datamaps&geo=Europe#Europe

[107] 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.

[108] Idem, cover letter.

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.[109]
The Customer Data may be routed through other locations during transfer and may also be processed in other regions. Microsoft has explained that processing can occur at any location where Microsoft operates (except for China, since this is a completely separate cloud). This also applies to the replications of the data (colloquially known as backups). This will be explained in paragraph 10 *Retention Periods*.

Access to the Customer Data that Microsoft defines as Core Online Services is audited following the strict controls of SOC-2. Access to the Customer Data provided by Office 365 ProPlus is audited following the ISO 27001 norms. There is no public documentation about audit on the diagnostic data collected through Controller Connected Experiences and the mobile Office apps.

Paragraph 2 of this report describes the different kinds of diagnostic data that are generated through respectively the mobile Office apps, the use of Office Online, the use of the cloud storage and mail services and the Connected Experiences. As explained in paragraph 2 of this report, the diagnostic data from the different Office 365 products and services are sent to, or collected directly on, Microsofts servers in the USA. The network end points that Privacy Company has observed for the traffic from the mobile Office apps are also in the USA, including the traffic to marketing company Braze.

Microsoft publishes two lists of network endpoints, for the Windows consumer and professional versions, and for the Windows Enterprise versions.[110] Both lists contain network endpoints for Office diagnostic data, such as onecollector.cloudapp.aria, v10.events.data.microsoft.com and watson.telemetry.microsoft.com.

The data can be analysed everywhere where Microsoft has computing capacity. Microsoft does not want to commit to storage of diagnostic data in the EU, as that would only be a cosmetic solution. The diagnostic data are analysed and processed in the USA, and are processed in a short-term database (30 days) and a long-term database (18 months). See paragraph 10 for the description of the retention periods.

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, of Office Online, of the Connected Experiences and of the connected cloud e-mail and storage services. These are the diagnostic data.

As explained in the introduction and paragraph 2.2, Privacy Company has analysed the telemetry events from the mobile Office apps. The telemetry clients inside the mobile Office apps collect events about the usage of the software and stores these snapshots on the device. Similar to the way in which Microsoft collects telemetry

[109] 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.

[110] Microsoft, Windows endpoints non-enterprise editions, URL: https://docs.microsoft.com/en-us/windows/privacy/windows-endpoints-1903-non-enterprise-editions and Windows 1903 Enterprise endpoints, URL: https://docs.microsoft.com/en-us/windows/privacy/manage-windows-1903-endpoints.

data about the use of Windows 10 and Office 365 ProPlus, the company encodes the telemetry data about the use of Office in an unknown binary format.

Each encoded packet contains multiple events that occurred over a period of time. This practice reduces the number of packets that are sent from the mobile apps to Microsoft, to limit the use of the end-user's device resources.[111]
It is not known how frequently the software captures data, or how frequently the client transmits the collected data to the Microsoft servers. As shown in **Appendix 1** with this report, some events such as 'scenarios' from the Teams app contain many different fields. This event was sent 1.055 times in the short time span of performing the scripted scenarios (less than 1 hour) on the device.

Technically, the diagnostic data from the mobile Office apps were observed to be transmitted to two endpoints in the USA.[112] vortex.data.microsoft.com and mobile.pipe.aria.microsoft.com. The first endpoint was observed only from PowerPoint on iOS, not from other applications and not from Android.

Microsoft also collects content data. Microsoft collects file and path names from files via the system-generated server logs on the cloud servers, when using SharePoint Online and OneDrive for Business. Microsoft also collects content data from the content of files, emails or chats when a user uses a Connected Experience, such as a spelling checker. Finally, as a cloud provider, Microsoft collects every letter a user enters and stores in the online text, collaboration, presentation and calculation programs that are stored in the cloud storage services, or sent via Exchange Online. The latter processing falls outside the scope of this DPIA report.

At present, the collection of diagnostic data is not transparent. Apart from the lack of a Data Viewer Tool for the mobile Office apps, Microsoft does not actively inform data subjects and admins about the diagnostic data processing, not in the apps, not in the application setting options when using a browser and not on its general information pages.

As described in paragraph 3.1 (*Privacy choices in Office Online and the mobile Office apps*) Microsoft also does not (yet) offer any options for minimizing the data flow in the mobile Office apps.

8.1 Local versus hybrid cloud use of Office software

Government organisations can use the Office Online software and the mobile Office apps in two different ways.

1. With *on-premises* storage of data
2. With a hybrid set-up.

In the first set-up the data storage is *on-premise*, in the governmental data centres. The Dutch government is also testing a hybrid cloud combination. In this new, second, set-up, users can use online storage in SharePoint Online and OneDrive for Business, and use additional Office 365 cloud services such as the Online Exchange server and Skype.

From a data protection perspective, the main difference between the different Office deployments is that users must always have a Microsoft Enterprise account, except in case the installation is completely local (first scenario). In that case Microsoft does not know the local ID. However, if a user with a local account wants to use the

[111] Microsoft confidential response to the first Office 365 ProPlus DPIA report, 24 September 2018, p. 6.
[112] Meeting report 28 August, answer to Q7.

Online Exchange mail server, or the Connected Experiences, (an association with) a Microsoft account is required.

In the first scenario, Microsoft collects telemetry data from the in-built telemetry client in the mobile Office apps, and diagnostic data from its cloud servers relating to the use of Office Online and the Connected Experiences.

In the second scenario, Microsoft collects additional personal data through system-generated server logs related to its cloud storage and mail services. In the second scenario, the use of the Azure AD is required.

8.2 Azure AD logs and usage data

In addition to the diagnostic data about the use of Office Online, the mobile Office apps, the Connected Experiences and the cloud storage services, Microsoft collects and processes two types of personal data 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, user analysis, software debugging, system health analysis and system-wide analysis using 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.

Microsoft writes: "*Log files contain data about usernames, groups, devices, and apps. Log files are originally created and stored in Azure storage in the data center where the Azure AD service runs. 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 centres in the Continental United States.*"[113]

In addition, Microsoft describes that it collects a category of 'Usage data' on the Azure AD. Not only for the customers, but also for themselves, in order to analyse system usage and to be able to improve the service. Microsoft says that it will first delete the personal data in 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.*"[114]

The removal (deletion or destruction) of identifying data after its collection is a processing of personal data. The GDPR applies to this. The fact that Microsoft deletes certain personal data from the log files does not make any difference in the assessment that Microsoft processes personal data via these log files.

8.3 Big data processing

[113] Microsoft, Azure Active Directory Data Security Considerations - Download Center, http://download.microsoft.com/download/A/A/4/AA48DC38-DBC8-4C5E-AF07-D1433B55363D/Azure-AD-Data-Security-Considerations.pdf

[114] Ibid.

Until May of 2019, Microsoft did not provide comprehensive documentation about the content of the diagnostic events collected by the use of the Office 365 ProPlus software and Connected Experiences. Microsoft has also explained that until recently, there were no central rules governing the collection of telemetry data.[115] Since 2018, there are rules, 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."* [116]

Microsoft has not provided information about rules governing the collection of information through the Connected Experiences or through the mobile Office apps.

Microsoft stores the telemetry data from Office and Windows together with diagnostic data from its cloud services in the central long-term database Cosmos.

A former Microsoft engineer explained the architecture of Cosmos in a slideshow, and wrote that Cosmos not only contains these diagnostic data, but also data from Skype, Xbox, Bing, Ads and more.[117] The engineer explains: "*Teams put their data in Cosmos because that is where the data they want to join against is*", and: "*Cluster size exceed 50.000 servers.*"[118]

In an earlier presentation from 2011 two former Microsoft engineers explained:
"*We ingest or generate a couple of PiB every day*
- *Bing, MSN, Hotmail, Client telemetry*
- *Web crawl snapshots*
- *Structured data feeds*
- *Long tail of other data sets of interest*"[119]

In view of the outgoing data traffic to marketing company Braze from at least three iOS apps, as described in paragraph 2.2 of this report, Microsoft could possibly receive profiles from this company, and combine this with the diagnostic data as 'data sets of interest'. As quoted in paragraphs 4.3.10 and 4.3.11 of this report, Microsoft contractually permits itself to analyse data from different sources to predict interests and to send users 'relevant offers' and show targetted advertisements in Microsoft products and services, and on third party websites.

Microsoft can collect new events on the fly, both through its own cloud servers as well as through the telemetry clients. Therefore, any inspection of the diagnostic data remains a snapshot. The data processing remains dynamic.

[115] Meeting report 28 August 2018, answer to Q1.
[116] Microsoft confidential response to first Office 365 ProPlus DPIA report, 24 September 2018, p. 10.
[117] Presentation from Eric Boutin. Meetup from 5 November 2015, URL: https://www.slideshare.net/MemSQL/how-microsoft-built-and-scaled-cosmos (URL last visited and recorded 12 July 2019)
[118] Ibid, slides 8 and 13.
[119] 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 and recorded 12 July 2019).

9. Additional legal obligations: ePrivacy Directive

In this paragraph, only the additional obligations arising from the ePrivacy Directive are discussed. Given the limited scope of this DPIA, other legal obligations or policy rules (for example with regard to security), are not included in this report.

As outlined in the investigation report of the Dutch DPA about Windows 10 telemetry data, additionally certain rules from the current ePrivacy Directive may apply to the placing of information 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.

The consequences of this provision are far-reaching, since this provision requires clear and complete information to be provided *prior* to the data processing, and it requires consent from the user. In part B of this DPIA the difficulty is assessed of obtaining freely given consent from employees, given their dependency in the relationship with their employer.

The current ePrivacy Directive (as implemented in the Netherlands in Chapter 11 of the Telecommunications Act) also contains rules on the confidentiality and destruction of data from the content and on communication behaviour. Article 5(1) obliges the Member States to guarantee the confidentiality of communications and related traffic data via public communications networks and public electronic communications services. Article 6(1) obliges providers of public telecommunications services to remove or anonymise the traffic data as soon as they are no longer necessary for the transmission of the communication. Although this ePrivacy Directive does not apply to providers of software in the cloud (which always involves communication via a public electronic communications network), the future ePrivacy Regulation is likely to make these rules applicable to Microsoft as a provider of e-mail and voice services.[120]

On 10 January 2017, the European Commission published a proposal for a new ePrivacy Regulation.[121] The proposed Article 8(1), *Protection of information stored in and related to end-users' terminal equipment*, expanded 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 view on 23 October 2017.[122] It added a specific exception on the consent requirement to provide updates as well as an

[120] See also recital 22 in the ePrivacy Directive 2002/58/EC, revised in 2009 by Directive 2009/136/EC: "*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*."

[121] 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.

[122] Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)) Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Marju Lauristin, URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0324+0+DOC+XML+V0//EN#title8.

exception regarding employees. To Article 8(1) 2 new exceptions on the consent requirement were added.

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;
And
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 of the EU Member States has been debating the proposal since October 2017.[123] In a draft published 19 October 2018, the ministers proposed an exception for software updates, not limited to security updates, similar to the exception proposed by the European Parliament. The ministers also intended to allow employers to seek the consent of employees, without any considerations about the conflict this would cause with the presumption in the GDPR (Art. 7(4) and Recital 43) that consent cannot be freely given where there is a clear imbalance between the data subject and the controller.

This proposal for Article 8 of the ePrivacy Regulation has not been changed in the most recent publicly available document with the outcomes of the deliberations in the Council, published 12 July 2019.[124] The Council proposes to rename Article 8 to: *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 software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:
(…)
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;[125]

[123] The file number for the Council is 2017/0003 (COD). The developments can be followed via https://eur-lex.europa.eu/procedure/EN/2017_3.
[124]. Council of the European Union, Interinstitutional file 2017/0003 (COD), Brussels 12 July 2019, 11001/19 URL: https://www.parlament.gv.at/PAKT/EU/XXVI/EU/07/15/EU_71514/imfname_10916407.pdf.
[125]. Council report 19 October 2018, URL: https://www.parlament.gv.at/PAKT/EU/XXVI/EU/03/91/EU_39172/imfname_10848802.pdf. The proposal remains unchanged in the last complete draft of 12 July 2019.

The Council also proposes to insert an exception for security purposes in the use of electronic communications data, in Art. 6 (*Permitted processing of electronic communications 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;
(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.

With regard to employees, the Council proposes to add the following explanation in recital 19b (but not in Article 6 or 8):

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 entity having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service. In such case, consent needs to be obtained from the individual concerned.

The Council provides more explanation about the consent requirement in the new recital 21: [126]

Use of the processing and storage capabilities of terminal equipment or 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 necessary and proportionate for the purpose of providing a specific service, such as those used by IoT devices (for instance connected devices like connected thermostats), 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.
(…)
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 is likely that the ePrivacy Regulation will contain prolong the existing rules about the consent requirement prior to the placing or retrieving of information from end-user devices, and will contain a limited exception on the distribution of automated updates to end-users.[127]

[126] Ibid.
[127] It is not clear when the ePrivacy Regulation (2017/0003/COD) will be adopted or enter into force. Progress can be followed through https://eur-lex.europa.eu/procedure/EN/2017_3. Early July 2019, the ministers of the Member States represented in the Council have not yet reached agreement.

10. Retention Periods

The Enrolment documents, including the OST, do not mention the retention periods of diagnostic data. In the OST Microsoft only makes a commitment for the retention period of Customer Data. Microsoft states it will retain Customer Data for 90 days after the end of the subscription, and delete it within an additional 90 days.

Since 6 May 2019, Microsoft has been publishing information about the various retention periods of personal data in Office 365.[128] Microsoft distinguishes between Customer Content (all text, sound, video, image files, and software created and stored in Microsoft data centres when using the services in Office 365), other Customer Data and Personal Data that are not part of the Customer Data.

Microsoft also distinguishes between active and passive deletion of data. Passive deletion occurs if a tenant ends the subscription; active deletion when a user deletes data, or an admin deletes a user.

Microsoft overview of personal data and retention periods

Customer Content	**Active Deletion** at most 30 days, **Passive Deletion** at most 180 days after termination of the subscription
Data that identifies or could be used to identify the user of a Microsoft service. EUII does not contain Customer content	At most 180 days in case of active deletion by the admin and passive deletion after termination of the subscription
End User Pseudonymous Identifiers (EUPI)	**Active Deletion** at most 30 days**, Passive Deletion** at most 180 days after termination of the subscription

The table indicates that diagnostic data are stored between 30 and 180 days. However, this table is far from complete.

Discussions between SLM Rijk and Microsoft have clarified that Microsoft's middle row of data includes all system-generated event logs, which it 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.

The updated table does not provide any explanation about the retention of system-generated event logs or telemetry events from the mobile Office apps. Microsoft has confirmed that the personal data in the system-generated event logs are treated like EUII and will similarly be stored up until half a year after the end of subscription.[129]

Microsoft mentions System-generated Log Data in its *Guidance for data controllers to conduct a Data Protection Impact Assessment*, and explains they are stored for a period of half a year: "*This data is retained for a default period of up to 180 days*

[128] Microsoft, Data Retention, Deletion, and Destruction in Office 365, 6 mei 2019 (niet beschikbaar in het Nederlands), URL: https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-data-retention-deletion-and-destruction-overview.
[129] Microsoft confidential answer 1 October to the 10 follow-up questions, answer to Q4b.

from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations."[130]

Microsoft has provided SLM 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 sub processors 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 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.*"[131]

Microsoft does not offer a possibility to delete outdated diagnostic data from Office 365 ProPlus, Office Online 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 Office, and eliminate its Azure Active Directory presence.[132]

[130] Data Protection Impact Assessments: Guidance for controllers using Microsoft Office 365. Available at https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpia-Office 365 (URL last visited and recorded on 8 July 2019).
[131] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q8 (preamble).
[132] Ibid, answer Q8b.

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.[133] 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.*"[134] In its GDPR compliance assessment 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.

SharePoint Online does not perform system-level backups. Daily incremental and weekly full backups are conducted for SQL Server schemas, and Active Directory information is backed up through replication across sites and datacenters. SQL Server schemas are stored for no less than 30 days and geo-replicated to alternate datacenters for high availability.
Standard images and scripts are used to recover lost servers, and replicated data is used to restore customer user-level data."[135]

[133] Meeting report 30 August 2018, answer to Q33.
[134] Microsoft, Data Retention, Deletion, and Destruction in Office 365, 6 May 2019.
[135] Microsoft Compliance Manager Office 365, tab 'Microsoft Managed', Control ID: 6.9.2 'Information backup'. Accessible (with Microsoft account log-in) via the Microsoft Servicetrust dashboard, the Compliance Manager, URL: https://servicetrust.microsoft.com/FrameworkDetailV2/b3d8589d-5987-45b7-8591-235c4a2f2ca2.

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.

As analysed in paragraph 5.1 of this report, as a result of the negotiations with SLM Rijk, Microsoft behaves as a data processor for most of the diagnostic data processing (Office Online, the Processor Connected Experiences and the cloud storage and e-mail services). In its role as data processor, Microsoft can rely on the relevant legal grounds of the Dutch government organisations for the data.

However, Microsoft acts as a data controller for the mobile Office apps and the Controller Connected Experiences. This means that none of the contractual improvements negotiated by SLM Rijk apply to the processing of diagnostic data from these apps and services. As described in paragraph 5 of this DPIA report, Microsoft contractually permits itself to process the diagnostic data for 14 purposes from its Privacy Statement. Since government organisations cannot centrally block access to these services for Office Online and the mobile apps, they are joint controllers with Microsoft for the processing of these diagnostic data.

In its Privacy Statement Microsoft states that the processing for these 14 different purposes may be based on different legal grounds, but the company does not specify the legal ground for each of the different purposes. "*We rely on a variety of legal reasons and permissions ("legal bases") to process data, including with your consent, a balancing of legitimate interests, necessity to enter into and perform contracts and compliance with legal obligations, for a variety of purposes*".[136]

Below, the different possible legal grounds are assessed for the different purposes of the processing. The ground of vital interest is not discussed since nor Microsoft nor the Dutch government organisations have a vital (lifesaving) interest in the processing of the personal data.[137] This paragraph does not distinguish between the roles of Microsoft as a data processor, and Microsoft as a joint controller: in both cases Microsoft needs to rely on the legal ground of the Dutch government organisations.

Independently of this, as specified in the contract with SLM 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.

[136] Microsoft Privacy Statement, Personal Data We Collect, June 2019.
[137] Microsoft mistakenly claimed in its initial response to the initial Office 365 ProPlus DPIA report that it could rely on the vital interest of data controllers as legal ground for the processing of personal data for security purposes. This legal ground only applies to matters of life and death and thus does not merit any further consideration in this report.

11.1 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*"

a. Government organisations as data controllers for the diagnostic data about Office Online, the processor Connected Experiences and the cloud storage and e-mail services

This legal ground is not applicable for the processing of the diagnostic data from Office Online and the mobile Office apps, including the Connected Experiences and cloud storage and mail services, because for employers it is almost impossible to obtain valid, freely given consent from employees, given the clear imbalance in the labour relationship.

Instead, employers should rely on the necessity of the processing to perform their (labour) contract with the employees. Employers should take into account that Article 7(4) of the GDPR adds a prohibition on asking for consent if the processing is not strictly necessary for the performance of the contract. Recital 43 of the GDPR explains: *"Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."*

b. Microsoft and government organisations as joint controllers for the diagnostic data about the mobile Office apps and optional (Controller) Connected Experiences.

If the administrators of the government organisations cannot centrally prohibit the use of the Controller Connected Experiences in Office Online and the mobile Office apps, and have no way of technically preventing that employees connect their work accounts in the mobile Office apps, employees are asked for consent by Microsoft the first time they access a Connected Experience or when they download the apps. See illustration 7 in this report.

To the extent that Microsoft would want to rely on consent, the question does not meet the legal requirements of consent, as it is not specific nor informed, nor unambiguous. With regard to the mobile apps, 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.

11.2 Processing is necessary for the performance of a 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*."

a. Government organisations as data controllers for the diagnostic data about Office Online, the processor Connected Experiences and the cloud storage and e-mail services

Government employees are provided with the Office products to be able to carry out the tasks included in their job description. As described in paragraph 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.

As a result of the negotiations, Microsoft has agreed to only process the personal data in and about Office Online, the processor Connected Experiences and the cloud storage and e-mail services for three authorised purposes and has limited the amount of personal data it collects. Hence, to the extent that the processing of the diagnostic data from these services is strictly necessary for the performance of the contract which the data subject has with the governmental organisation, the government organisation may successfully appeal to this legal ground.

b. Microsoft and government organisations as joint controllers for the diagnostic data about the mobile Office apps and the optional (Controller) Connected Experiences.

If Microsoft does not wish to base the diagnostic data processing on the consent of the employees, it is plausible that Microsoft assumes it can rely on the legal ground of contract. Microsoft could argue that employees would freely sign a separate contract with Microsoft by ticking the box to use the Controller Connected Experiences, or by downloading the Office apps from the Apple and Android appstores. Such an argument would be incorrect for multiple reasons.

First of all, employees have a contract with their employer, a Dutch government organisation, and not with Microsoft.

Second, even if checking a box to use a service or downloading an app without any information about the consequences in terms of personal data processing could possibly qualify in civil law as an intention to conclude an agreement, the processing does not meet the requirements of the legal ground of art. 6(1) b in the GDPR, the necessity to process specific personal data to perform a contract. As outlined above, absent comprehensive documentation about the nature, volume and specific purposes of the diagnostic data processing, Microsoft is unable to demonstrate the necessity of the processing of these data.

The European Data Protection Board writes in its draft guidelines on the legal ground of necessity for a contract: "*A controller can rely on Article 6(1)(b) to process personal data when it can, in line with its accountability obligations under Article 5(2), establish both that the processing takes place in the context of a valid contract with the data subject* ***and that processing is necessary in order that the particular contract with the data subject can be performed*** [emphasis added for this DPIA report].[138]

[138] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version for public consultation published 12 April 2019, URL: https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-Article-61b_en [Guidelines not finalised 22 July 2019].

In fact, as described in paragraph 8.3 of this report (*Big data processing*), Microsoft contractually permits itself to predict individual interests based on the diagnostic data, and present relevant offers and targeted advertisements to the government employees when it processes diagnostic data as a data controller. The EDPB repeats the earlier opinion of Article 29 Working Party that contractual necessity is not a suitable ground for behavioural advertising. *"As a general rule, behavioural advertising does not constitute a necessary element of online services. Normally, it would be hard to argue that the contract had not been performed because there were no behavioural ads. This is all the more supported by the fact that data subjects have the absolute right under Article 21 to object to processing of their data for direct marketing purposes.*

Further to this, Article 6(1)(b) cannot provide a lawful basis for online behavioural advertising simply because such advertising indirectly funds the provision of the service. Although such processing may support the delivery of a service, it is separate from the objective purpose of the contract between the user and the service provider, and therefore not necessary for the performance of the contract at issue."[139]

The requirement of strict necessity for all data and for all purposes is addressed in the next sections 13 and 14 of this report (purpose limitation and necessity).

Third, employees are not free to sign contracts with third parties to use functionalities, as they generally have no power or legal possibility to create a liability on behalf of their employer (part of the Dutch state).

Finally, the reseller agreements that Dutch government organisations use, that also apply to the reselling of Microsoft Office products, explicitly prohibit users from accepting and agreeing to general terms and conditions from vendors.[140] In this context it is highly unlikely that employees would be able to sign a contract with Microsoft that would give Microsoft a license, outside of the contractually agreed boundaries by the employer, to process personal data relating to that employee and other data subjects.

11.3 Processing is necessary to comply with legal obligation

Article 6 (1) (c) GDPR reads: *"processing is necessary for **compliance with a legal obligation** to which the controller is subject"*

a. Government organisations as data controllers for the diagnostic data about Office Online, the processor Connected Experiences and the cloud storage and e-mail services

This legal ground can only be invoked for specific purposes if these purposes have been laid down in the law. Though there is a general legal obligation in the GDPR to guarantee the security of personal data and to be able to detect security incidents,

[139] Idem, paragraphs 49 and 50, page 13.
[140] The tekst of these provisions in Dutch: ***Algemene en bijzondere voorwaarden***
8.1. De toepasselijkheid van algemene en bijzondere voorwaarden van Wederpartij dan wel van door Wederpartij bij het verrichten van de Prestatie te betrekken derden, is uitgesloten, tenzij daarvan in de Nadere overeenkomst expliciet wordt afgeweken.
8.2. De voor het gebruik van de Prestatie vereiste acceptatie van algemene of bijzondere voorwaarden, zoals bijvoorbeeld bij "shrink-wrap"- en "click-wrap" licenties, bindt Opdrachtgever niet. Wederpartij vrijwaart Opdrachtgever dat dergelijke acceptaties niet leiden tot enige beperking op het Overeengekomen gebruik.

which would be next to impossible without keeping (audit) log files, government organisations cannot successfully invoke this legal ground for the processing of diagnostic data for security purposes.

b. Microsoft and government organisations as joint controllers for the diagnostic data about the mobile apps and the optional (Controller) Connected Experiences.

Neither Microsoft nor the government organisations are subjected to any specific legal obligation to process diagnostic data about the use of the mobile Office apps and the optional Controller Connected Experiences.

11.4 Processing is necessary for the public 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*"

a. Government organisations as data controllers for the diagnostic data about Office Online, the processor Connected Experiences and the cloud storage and e-mail services

This legal ground is not applicable since the government could also carry out its tasks with different software from other companies. The specific type of diagnostic data processing is not necessary to perform the public tasks of government; there is no specific public interest served by using Microsoft services.

b. Microsoft and government organisations as joint controllers for the diagnostic data about the mobile apps and the optional (Controller) Connected Experiences s.

Microsoft mistakenly claimed in its response to the initial Office 365 ProPlus DPIA report that it could rely on the legal ground of necessity for the greater public interest in fighting cybercrime and identity theft. Since Microsoft is not government, nor a public organisation, it can never rely on this legal ground.

11.5 Processing is necessary for the legitimate interests of the controller or a third party

Article 6(1) f 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.*"

a. Government organisations as data controllers for the diagnostic data about Office Online, the processor Connected Experiences and the cloud storage and e-mail services

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).

b. Microsoft and government organisations as joint controllers for the diagnostic data about the mobile apps and the optional (Controller) Connected Experiences.

It follows from Microsoft's public documentation about the Controller Connected Experiences that Microsoft collects both information about user behaviour, as well as content of the communication (such as the content of Word documents for the LinkedIn Resume Assistant, and the queries entered into search engine Bing via Search). Both types of data can be very sensitive. Microsoft contractually permits itself to process these personal data for all 14 purposes from its Privacy Statement. Even though Microsoft could have a legitimate interest in using some of the diagnostic data from the Controller Connected Experiences for the purposes of technically providing the service, keeping the service up-to-date and secure, in the current circumstances Microsoft processes these data for 14 purposes. Because there is no purpose limitation, the rights and freedoms of data subjects clearly outweigh the legitimate interests of Microsoft.

Following the order of the Dutch government DPIA model, the necessity of the processing is separately assessed in paragraph 14 of this report. However, the legal ground of legitimate interest requires a double proportionality test; whether the processing is strictly necessary to achieve legitimate purposes, and whether the interest of the data controller outweighs the fundamental rights and freedoms of the affected data subjects.

Illustration 13: table with the different applicable legal grounds in the current circumstances

Purpose	**Legal ground**	**Government organisations as data controllers**	**Microsoft as data controller**
Providing the service, inc troubleshooting and bug fixing	Consent	X	X
	Contract	√	X
	Legal obligation	X	X
	Legitimate interest	√	√
Providing updates	Consent	X	X
	Contract	√	X
	Legal obligation	X	X
	Legitimate interest	√	√
Security	Consent	X	X
	Contract	√	X
	Legal obligation	X	X
	Legitimate interest	√	√
14 different purposes mobile Office apps and the Controller Connected Exp.	Consent	X	X
	Contract	X	X
	Legal obligation	X	X
	Legitimate interest	X	X

There is an additional problem with the requirements of Article 5(3) of the ePrivacy directive (Article 11.7a Tw in the Netherlands). According to this law, prior user

consent is required if a company stores data on a data, and makes the device send these data via the internet to that company. Preceding the analysis of necessity, the special character of the diagnostic data from the mobile Office apps and the ePrivacy consent requirements preclude further processing for most of the purposes without the explicit consent of the end-user. However, as analysed above, employees are not free to give consent for other purposes.

In sum, as a result of the purpose limitation, the government organisations as data controllers can invoke the legal grounds of necessity to perform a contract and for their legitimate interest for the diagnostic data processing by Microsoft for the three authorised purposes.

However, these legal grounds are not available for the processing of diagnostic data from the mobile Office apps and the Controller Connected Experiences. As joint controllers, Microsoft and the government organisations cannot rely on consent either given the dependency in the relationship between employees and employers. As Microsoft does not offer technical possibilities to prohibit employees from using the mobile Office apps and the Controller Connected Experiences through Office Online and the mobile apps, they can only warn their employees not to use these services.

12. Special categories of data

As explained in paragraph 2.6.1 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.

If that is the case, 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) requires additional measures, such as encryption. 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 authorized 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.

Similar risks may apply to other categories of sensitive personal data, 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."[141]

The EDPS refers to the criteria provided by the Article 29 Working Party when a Data Protection Impact Assessment (DPIA) is required.[142] The 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.

Even though Microsoft guarantees that the Customer Data are stored in data centres in the European Union, these guarantees do not apply to the diagnostic data. Those are transferred directly to Microsofts servers in the USA.

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 sub processors, and (iii) through hostile state actors.

If a government organisation processes special categories of data, it should have the technical ability to prohibit the use of the optional (Controller) Connected Experiences. There is no exception in the Articles 9 and 10 of the GDPR that applies to the prohibition of the processing of these personal data by Microsoft for its own 14 purposes. The only general useful exception in Article 9 GDPR is if the data subject has given explicit consent. Article 10 of the GDPR completely prohibits the processing of personal data relating to criminal convictions and offences, if not only under the control of official authority or when authorized by Union or member law.

As described in paragraph 5.2, Microsoft and the government organisations that cannot prevent the use of the optional (Controller) Connected Experiences and the mobile Office apps are joint controllers for these diagnostic data. Since nor Microsoft nor the government organisation are able to obtain freely given (and specific and informed) consent, they certainly cannot meet the higher threshold of 'explicit' consent.

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.

[141] 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

[142] Article 29 Working Party, 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 .

Purpose limitation is the most difficult principle to comply with in big data processing. Further processing for research purposes can possibly be based on Article 89 of the GDPR, but only if strict guarantees are in place, such as the use of anonymous data. 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.

As described in paragraph 4.1 of this report (*Results of negotiations purpose limitation with Microsoft*), Microsoft has agreed with SLM Rijk to act as a data processor for the Online Services and limit the data processing to three authorised purposes, and only where proportional. This is highly relevant for the diagnostic data processing through Office Online and the cloud storage and e-mail services. Use of personal data for profiling, data analytics, market research and advertising purposes has been explicitly forbidden in the contract with SLM Rijk, for both the content data and the diagnostic data. Microsoft has also made a major effort in the last 7 months to inform users about the categories of personal data and specific purposes for which Microsoft uses the diagnostic data from Office 365 ProPlus.

Unfortunately, these purpose limitation do not apply to the processing of diagnostic data from the mobile Office apps and the Controller Connected Experiences. Microsoft contractually permits itself to process these personal data for 14 purposes from its Privacy Statement. Microsoft equally has not published public documentation about the contents and specific purposes for the processing of these diagnostic data.

As described in paragraph 2.2 Microsoft allows at least three of its iOS mobile Office apps to send identifying data to the US-based marketing company Braze. This company is specialised in predictive profiles. Such profiles could very well be used to send the employees 'relevant offers' and targeted advertising.

As quoted in paragraph 4.3.1 of this report, Microsoft contractually permits itself to determine what purposes it deems *compatible* with the purpose of providing the service. As quoted in paragraph 6.2 of this report, about Microsoft's interests in the data processing, Microsoft focusses on the perceived needs of the millennial age group of users. Microsoft is concerned that they may switch any time to a 'free' service if they are not reminded of the Office functionalities. Microsoft therefore wants to present targeted recommendations on screen in the Office applications. This specific form of advertising has been explicitly prohibited in the amended contract with SLM Rijk, but only regarding the online services for which Microsoft acts as a data processor.

The two examples show that the purposes for which Microsoft can process the diagnostic data from the Controller Connected Experiences and the mobile Office apps are too broad to effectively allow the government organisations to be in control over the purposes for which their data could be processed.

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. It has to be assessed whether the same purpose can reasonably be achieved with other, less invasive means. If so, these alternatives have to be used.

Second, 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 amount of personal data processed should be decreased to what is necessary.

Therefore, essentially, the data controller may process personal data insofar as is necessary to achieve the 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.[143]

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 of their data being processed, that the legal conditions for data processing are all adhered to, and that the principle of proportionality is respected.

Since May 2019, Microsoft publishes a lot of public information about the diagnostic data from Office 365 ProPlus. Since the release of the new version of Office 365 ProPlus on 29 April 2019, administrators have different options with regard to the Connected Experiences. Microsoft has also made its existing Data Viewer Tool for the telemetry data from Windows 10 capable of showing the telemetry data from Office 365 ProPlus. These are huge improvements to make the processing of diagnostic data more transparent, but the work is not completed yet.

Microsoft has not published any documentation about the diagnostic data collected through Office Online and the mobile Office apps. There is a similar lack of transparency about the diagnostic data collected through the processor and controller Connected Experiences. Microsoft only provides five examples of events collected on the end-user device that send service diagnostic data to Microsoft.[144]

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

[144] Microsoft, Overview of privacy controls for Office 365 ProPlus, last updated 6 May 2019, Examples of events for service diagnostic data.

Microsoft does not provide an overview of the diagnostic data that are generated in system logs from Microsoft's servers that provide the Connected Experiences.

As Microsoft writes: "*We will be extending these new and improved privacy controls to additional Office clients, including Teams, Office for Mac, and our mobile 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.*"[145]

Though it is possible for data subjects to ask their administrator to perform a data subject access request through Microsofts DSR tool and a Content Search in the audit logs, these results do not contain any information about the diagnostic data collected via the Connected Experiences.

There is no public, centrally organised documentation about the diagnostic data collected via the system-generated logs about Microsofts own cloud storage and e-mail servers (SharePoint Online and OneDrive for Business and Exchange Online).

In sum, there is a lack of transparency about the diagnostic data processing through the mobile apps, the Connected Experiences and the cloud storage and e-mail services.

The principles of data minimisation and privacy by default demand that the processing of personal data is limited to what is necessary: Data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (Article 5 (1) (c) GDPR). This means essentially that data controller may not collect and store data that are not directly related to a legitimate purpose. Following this principle, the default settings for the collection of data have to minimise the data collection, have be set to the most privacy friendly settings. This is not the case for most settings with regard to Office Online and the mobile Office apps.

Different from the new versions of Office 365 ProPlus released since 29 April 2019, administrators do not have any choices with regard to the content and volume of diagnostic data from Office Online and the mobile Office apps.

There is no technical possibility to prevent the use of the Controller Connected Experiences in Office Online and the mobile Office aps. Equally, government administrators cannot technically prevent employees from using the mobile Office apps. As assessed in paragraph 11 of this report, Microsoft as a data controller does not have a legal ground for the processing of diagnostic data from these apps and services for most of the purposes from its Privacy Statement. Because the government organisations cannot prohibit the use of these services, they become joint controllers with Microsoft, and risk processing personal data for unlawful purposes.

In sum, possible usefulness (*nice to have*), does not meet the strict requirement of necessity. This is especially of concern with regard to the Controller Connected Experiences. These services explicitly collect content data through the system-generated server logs, such as a search result, or a look-up of data about that topic on the Internet, and Microsoft allows itself to process these data for a range of commercial purposes.

[145] Ibid.

The principle of storage limitation demands that personal data are only retained as long as necessary for the purpose in question. Data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*" (Article 5 (1) (e), first sentence GDPR). This principle therefore demands that personal data are deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller. The text of this provision goes on to clarify that "*personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject*" (Article 5 (1) (e), second sentence, GDPR).

As described in paragraph 10 of this report, the diagnostic data collected through the telemetry clients in the mobile Office apps are stored short-term for 30 days and in Cosmos up to 18 months, while the system-generated server logs are kept for half a year (180 days). It is hard to argue that the old telemetry data are necessary, adequate and relevant.

This long retention period is especially of concern with regard to the Controller Connected Experiences, given the lack of purpose limitation. With regard to the other diagnostic data, Microsoft only acts as a data processor, and has contractually guaranteed to the Dutch government that it will only process these personal data for the three authorised purposes, and only if proportionate. In view of this purpose limitation and the effective right to audit compliance with these purposes, and the fact that no content data or direct identifiers are included in the telemetry data, the diagnostic data processing for which Microsoft acts as a data processor is no longer disproportional.

With regard to the processing of diagnostic data through the Controller Connected Experiences and the mobile Office apps, the data processing does not comply with proportionality requirements given the lack of transparency, the absence of a technical opt-out and the real risk of unlawful further processing of the diagnostic data for advertising purposes.

14.3 Assessment of the subsidiarity

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

Prior to the contractual improvements achieved by SLM Rijk for Dutch government organisations in May 2019, Microsoft was of the opinion that government organisations were free to determine the purposes for which diagnostic data were processed, by (1) choosing whether or not to use the product, and (2) to determine the scope of the processing by selecting the appropriate settings.

In reality, the freedom to decide not to use Microsoft Office was limited or non-existent. In practice, government organisations have been working for a very long time with Microsoft Office. They have organised their work processes and development to integrate with Office software. Most government employees have never worked with other software in their life.

There are no directly equivalent software alternatives for Dutch government organisations. Alternative providers of work productivity software such as Google, or open source software such as Open Office or Libre Office, do not provide the exact

same functionality, nor can it be assumed they would present no or less data protection risks. A possible switch to either Google or Open Office would present serious difficulties in working with documents created in Office (for example lay out templates and track changes that do not convert without serious loss of usability). . Added to that there are the costs of migrating existing content, and redevelopment of specific applications that interact with the Office software. This situation can also be described as vendor lock-in.

An important reason for the government organisations to switch to Office 365 licenses (besides the end of technical support for older Office versions[146]), is the ability to enable employees to work at home and abroad with different devices. Because Microsoft acts as a data controller and does not allow administrators to technically prohibit the use of Office Online and the mobile Office apps, they effectively do not have a choice.

As a result of the negotiations between SLM Rijk and Microsoft, the known data protection risks relating to the diagnostic data processing in Office 365 ProPlus have been mitigated. No such guarantees can be given with regard to other elements of the Office 365 license, such as Office Online and the mobile Office apps.

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 Online 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 or 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 processes, together with information about the purposes of processing, recipients to whom data have been transmitted, the period for which personal data are to be stored, and information on their further rights as data subjects, such as filing a complaint with the Data Protection Authority.

[146] Organisations are forced to update to Office 365 in October 2020 at the very latest, as the support lifetime of older Office versions expires.

Microsoft undertakes "*to comply with reasonable requests from the Customer to assist in the Customer's response to such a request from the data subject. Microsoft declares that if it acts as a processor, it will forward a request to the data controller.*" [147]

As a data processor, Microsoft provides a tool for administrators to search and export all data that Microsoft considers to be a user's personal data. This tool is the Data Subject Request tool (DSR). As described in Sections 2.3 through 2.5 of this report, Privacy Company has used Microsoft's DSR tool to inspect information about the use of Office Online, the Connected Experiences and the cloud storage and e-mail services. It appears from the results of these access requests that Microsoft does not collect much data about the use of the Office Online applications. However, the diagnostic data about Office Online do not contain any data about the use of the Connected Experiences at all. This is remarkable, as Privacy Company made extensive use of different types of Connected Experiences in the test scenarios, insofar as these were available in the different applications in Office Online.

Another tool that Microsoft makes available as a data processor to all data controllers is the audit logfile. According to Microsoft, the audit logs provide detailed information about product and service usage data contained in system-generated logs. The audit logs are created by Microsoft for security purposes, and provide a view for the user to access product and service usage data contained in the system-generated event logs. 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.[148]

Thus, when a data subject exercises her rights under the GDPR, and requests access to her personal data, he or she can receive access to many data via the administrators, via the DSR and the audit logfiles, but not to any of the data about the Connected Experiences used in Office Online or the mobile Office apps.

Because Microsoft considers itself to be the (sole) data controller for the data processing regarding the use of the mobile Office apps and the Controller Connected Experiences, it does not provide access to the government administrators. Microsoft explains that employees should file a separate data subject request to Microsoft to obtain access to personal data collected through the use of these services. This can be done via the online (consumer) contact form, under 'Report a privacy concern'. Microsoft engages to "*comply with reasonable requests by Customer to assist with Customer's response to such a data subject request*."[149] Microsoft does not mention any possibility to view the diagnostic data traffic about the mobile Office apps in its in its DSR manual.

[147] Microsoft OST May 2019, p. 8.
[148] Microsoft, Office 365 Data Subject Requests for the GDPR, URL: https://docs.microsoft.com/en-us/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.*"
[149] OST May 2019, p. 8.

In sum, when data subjects exercise their access rights under the GDPR they only obtain information about the use of Office Online and the cloud storage and e-mail services. Microsoft does not provide access to the log files that it processes via the Azure Active Directory, to the diagnostic data regarding the use of the mobile Office apps and to the files that it generates as a result of the use of the Connected Experiences, including the Processor Connected Experiences.

Right of rectification and erasure
Thirdly, data subjects have the right to have inaccurate or outdated information corrected, incomplete information completed and - under certain circumstances - personal information 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.

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.[150] 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.[151]

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 Online, 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.

When Microsoft decides to show or to withhold 'relevant offers' or targeted advertising based on the diagnostic data from the mobile Office apps or the Controller Connected Experiences for which it considers itself to be a data controller, such an automated decision also generally does not produce legal effects. Unless there are exceptional circumstances such as discrimination based on ethnicity or price, such decisions also generally do not significantly affect the employees. Nonetheless, the wide range of purposes for which Microsoft contractually permits itself to process these data, may lead to extra risks for some employees. For example, if they regularly work with classified information, the collection of information about their locations and working hours via the mobile Office apps could lead to stalking or blackmailing.

Employees also have a right to data portability, if their personal data are processed based on the necessity to execute the (labour)contract. As outlined in the table in paragraph 11 of this report, the data processing for the three authorised purposes

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

can be based on this legal ground, namely, providing the service, inc troubleshooting and bug fixing, providing updates and security.

It is not clear though to what extent employees would be allowed to individually transfer data created in working hours, for the government, to another provider. Government organisations can plausibly claim they rather rely on their legitimate interest for the processing of these personal data. In that case, the right to data portability does not apply. Subsidiarily, with regard to the legal ground of contract, the provision of the data to the (former) employee would be in violation of the confidentiality principle (the exception in Article 23 (1) under i of the GDPR.

On the other hand, the government organisations are in charge of the contract with Microsoft, and they should be able to transfer the personal data relating to their employees collectively to another provider. Microsoft acknowledges this right, as part of a coalition of USA based providers called the Data Transfer Project. This initiative includes Facebook, Google, Microsoft and Twitter.[152]

In its own press release, Microsoft states that it is up to the Enterprise customer to provide data: "*Focus on a user's data, not enterprise data: Data portability needs to focus on data that has utility for the individual user such as content a user creates, imports, or approves for collection or has control over with the data controller service provider. Data portability for organizations are to be controlled by the organizations' own policy over their data.*"

Last, as part of their obligation as joint controllers, the government organisations must inform their employees/workers about the right to lodge a complaint, internally with the data protection officer, and externally with the Dutch data protection authority.

In sum, nor Microsoft nor the government organisations are currently able to (fully) honour the data subject rights.

[152] Big tech firms agree on 'data portability' plan, 20 July 2018, URL: https://phys.org/news/2018-07-big-tech-firms-portability.html. See also: https://blogs.microsoft.com/eupolicy/2018/07/20/microsoft-facebook-google-and-twitter-introduce-the-data-transfer-project-an-open-source-initiative-for-consumer-data-portability/

Part C. Discussion and Assessment of the Risks

This part concerns the description and assessment of the risks for data subjects related to the processing of diagnostic data from Office Online 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 metadata and content in the diagnostic data. The risks are described for government employees and for other data subjects that interact with government organisations. Part D provides an analysis of the remaining risks after the mitigating technical, organisational, and legal measures taken by Microsoft as a result of the negotiations with SLM Rijk.

16. Risks

16.1 Identification of Risks

The processing of personal data about the individual use of Office Online 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, e-mails and chats for Microsofts own purposes.

16.1.1 Metadata

Both Microsoft and the government organisations can use the collected diagnostic data about the user behaviour in Office Online 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 the Connected Experiences.

Microsoft contractually commits to the highest level of confidentiality for the content data it processes through the Online Services, the Customer Data. As a result of the negotiations between SLM Rijk and Microsoft, Microsoft has agreed to process all personal data, regardless whether it is content or metadata, only for the three authorised purposes, and only where proportionate. Microsoft has also agreed to never use these personal data, for which Microsoft is a data processor, for any type of profiling, data analytics, market research or advertising.

These contractual improvements prevent Microsoft from using the data from Office Online to distill a picture or create a profile of a person or to use the diagnostic data for advertising purposes. However, this guarantee does not apply to the mobile Office apps for devices with iOS or Android operating systems. As described in paragraph 2.2, separate from the telemetry events, outgoing post requests were observed in the captured traffic from the iOS apps PowerPoint and Excel to a domain belonging to the US-based marketing company Braze. The traffic allows Braze to observe that a unique user, with a unique device ID, has worked with a Word, PowerPoint or Excel file on an iOS device for a period of time in milliseconds. Although this information in itself does not reveal any sensitive data, the information is transferred to a company in the USA that is not bound by any of the privacy guarantees from Microsoft, and which is specialised in creating predictive profiles of individuals for commercial purposes.

Although the volume and content of the diagnostic data from the mobile Office apps and Office Online are limited compared to the diagnostic data from Office 365 ProPlus, the diagnostic data reveal information about the frequency and exact times of use of the Office Online applications and the times and frequency of usage of the mobile Office apps. Microsoft and the government organisations can additionally use the detailed activity logs of the use of the cloud storage services, with information about the individual log-in behaviour, e-mail behaviour and software usage. Last but not least, Microsoft can use the profiles created by the marketing company Braze.

The knowledge that Microsoft and the government organisations can process these diagnostic 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.[153] government employees may 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 e-mail to a friend or family member. The knowledge that the marketing company Braze is observing users' behaviour through the mobile Office apps with the purpose of creating a predictive commercial profile, can also have a negative impact on employees, since the resulting profile at Braze is not protected by any of the GDPR guarantees and could be traded and/or used for other purposes.

Government organisations can use these data for a negative assessment of and employee, if such usage is not explicitly excluded in the employee Privacy Statement. 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. Therefore it is essential that access 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).

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."[154]

There is an additional risk for some types of government employees if the metadata from for example storage of documents in SharePoint Online reveal that they are regularly working with classified or otherwise government sensitive materials. The

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

employees may become the targets of spear phishing, social engineering and blackmailing by foreign law enforcement authorities if Microsoft, or a sub-processor of Microsoft is ordered to hand over some of these data.

Communication and behavioural patterns may be analysed by foreign law enforcement authorities and/or intelligence services if Microsoft, or a sub-processor of Microsoft, is ordered to hand over some of these data. The transfer of data from the EU to the USA without a mutual legal assistance treaty (MLAT) as required in Article 48 of the GDPR, or other specific exception as defined in Article 49 of the GDPR, would be in breach of confidentiality requirements and the fundamental right to protection of communication secrecy. Additionally, such analysis may breach government secrecy classifications.

16.1.2 Content

Microsoft collects content data about the use of Office Online and the mobile Office apps in three different ways, when they are combined with the use of the Connected Experiences and the cloud storage services. First, Microsoft collects these data about the use of SharePoint Online and OneDrive for Business via its system-generated server logs on its cloud servers. Secondly, Microsoft collects the contents of documents for which the spelling is checked or of which parts are translated (through the Connected Experiences). Thirdly, as a cloud provider Microsoft collects every character that a user enters or stores in the online text, collaboration, presentation and calculator programs (the Customer Data). This last type of processing is out of the scope of this DPIA, but is nonetheless relevant to mention since prior to the negotiations with SLM Rijk Microsoft only gave assurances with regard to the Customer Data. Microsoft did not give explicit assurances with regard to the content data that are collected as a result of using the Online services.

Even though Microsoft has a policy stating that diagnostic data should not include content, these content data are included in the system generated event logs that are generated through the use of the cloud storage services SharePoint Online and OneDrive for Business. As explained in paragraph 2.5 of this report these log files contain file names and path names of documents. As result of the negotiations with SLM Rijk, Microsoft as data processor may only process these personal data for the three authorised purposes and can no longer itself determine other purposes that it would consider compatible with the main purpose of providing the service.

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. Similar to the metadata, there is an additional risk for some types of government employees if the file and path names reveal classified or otherwise sensitive government materials.

Such information could end up in the wrong hands, and thus be processed unlawfully through for example spear phishing, social engineering, and blackmailing. Additionally, there is a risk that law enforcement authorities demand access to these data from Microsoft, or a sub-processor of Microsoft.

Since May 2019, Microsoft provides most of the Connected Experiences as a data processor. Nonetheless, there 14 optional Connected Experiences for which Microsoft remains a data controller. Although there is a central opt-out policy for these Controller Connected Experiences in Office 365 ProPlus, no such opt-out has been created in Office Online or in the mobile Office apps.

Microsoft contractually permits itself to process the diagnostic data that result from the use of these Controller Connected Experiences 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.

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. [155]

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 transparency: inability to exercise data subject rights

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 Online, the mobile Office apps, the Connected Experiences and the system-generated event logs about the use of SharePoint Online and OneDrive for Business.

The Data Viewer Tool for Windows 10 and Office 365 ProPlus cannot be used to decode the telemetry events from the mobile Office apps.[156] The technical inspection of the outgoing data, as described in paragraph 2.2 of this report, shows that Microsoft does not collect many different kinds of diagnostic data (88 different telemetry events have been observed). The inspection also shows that Microsoft does not collect content data from the contents of files, e-mails or chats nor any file or path names. However, the inspection also reveals that at least three of the iOS apps (Word, PowerPoint and Excel) secretly send diagnostic data to the US-based marketing company Braze, without any information about the existence and purposes of this data processing. Since this traffic is invisible to the average 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.

Microsoft has not yet published public, centrally organised and detailed documentation about the diagnostic data collected via the system-generated logs about Microsofts own cloud storage (SharePoint Online and OneDrive for Business). There is a similar lack of transparency about the diagnostic data collected through the Processor and Controller Connected Experiences. Microsoft does not provide a limitative overview of the diagnostic data that are generated in system logs from Microsofts servers providing the Connected Experiences. The only way to get

[155] 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/.
[156] Obviously, the Data Viewer Tool cannot be used for Office Online, since this is a browser based service, and all data are collected on Microsofts own cloud servers.

information about the nature of this data processing, is via a data subject access request via Microsofts DSR tool, or by creating an audit log with activities stored by Microsoft relating to individual use of the online services. However, Microsoft did not provide any information about the use of either type of Connected Experiences in the data subject access requests.

The results of the DSR requests show that Microsoft does not collect many diagnostic data about the use of Office Online, and no content data from the contents of files, e-mail or chats, nor any file or path names. Hence, the data protection impact for government employees resulting from the processing of usage data of Office Online can be assessed as low. Although the risks for data subjects are higher when Microsoft does process content data, such as file and path names stored in the log files about the use of SharePoint Online and OneDrive for Business, and the contents of documents which are processed through the Processor Connected Experiences, the occurrence of the risks of loss of control and unlawful (further) processing remains low, since Microsoft as a data processor has agreed with SLM Rijk to only process these personal data for the three authorised purposes.

Nonetheless there are two remaining high risks resulting from the lack of transparency, the first with regard to the mobile Office apps and the second with regard to the (lack of access to) the Controller Connected Experiences

a. No information about further processing by US-based marketing company
As described in paragraphs 2.2 and 16.1.1 of this report, Microsoft sends traffic from at least three of the iOS apps (Word, PowerPoint and Excel) to the US-based marketing company Braze. This company is specialised in creating predictive profiles of individuals for commercial purposes and is not bound by any of the privacy guarantees from Microsoft. Because of the lack of transparency and lack of a consent question, users are unable to exercise a choice whether to provide informed consent. They are thus prevented from exercising their fundamental rights, such as the right to object against profiling and the right to have their data deleted.

b. No access to diagnostic data Connected Experiences
As described in paragraph 2.4 of this report Microsoft did not provide access to the log files about the Connected Experiences when Privacy Company filed data subject access requests, regardless of their status as 'processor' data or 'controller' data. Since Microsoft also does not publish extensive documentation, data subjects cannot know what diagnostic data Microsoft processes about them via the Controller Connected Experiences, and are thus unable to exercise their fundamental data protection rights.

In both cases, the impact on data subjects of this lack of transparency must be qualified as serious, due to the inability to exercise fundamental rights, while the chance of occurrence of both these risks is 100%. Therefore, they both result in a high data protection risk.

16.2.2 No technical opt-out Controller Connected Experiences and mobile Office apps: loss of control

In Office 365 ProPlus version 1904 and later, government organisations can turn off the Controller Connected Experiences. These controls do not exist for Office Online and for the mobile Office apps. Additionally, it is not possible for government organisations to prohibit employees from using the mobile Office apps.

Since May 2019, Microsoft has reorganised its Connected Experiences. Microsoft offers many frequently used services such as the Spelling Checker and the Translator as a data processor. There are 14 Connected Experiences for which Microsoft remains a data controller, which are related to the use of LinkedIn and Bing. Since version 1904 of Office 365 ProPlus, released on 29 April 2019, administrators can centrally block the use of the Controller Connected Experiences, and some or all of the Processor Connected Experiences. However, these controls are not available in Office Online and the mobile Office apps.

It is not clear if and when Microsoft will provide a similar control to administrators of Office Online and the mobile Office apps to block the use of the Controller Connected Experiences. Microsoft writes: "*We will be extending these new and improved privacy controls to additional Office clients, including Teams, Office for Mac, and our mobile 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.*"[157]

Additionally, it is not technically possible for government organisations to prevent their employees from downloading the mobile Office apps, unless they work with fully managed devices on which they can control all traffic (no "Bring Your Own Device"). The Office apps are freely available in the app stores, and there is no group policy or similar technical instrument to prevent employees from connecting with their work account in those apps.

Microsoft considers itself to be a data controller for the mobile Office apps and for the Controller Connected Experiences. Government organisations that make their employees work with Office 365 enable Microsoft to process the diagnostic personal data for its own purposes. Therefore, government organisations in practice become joint controllers with Microsoft for the processing of the diagnostic data about these services. Microsoft processes the data based on the consent of the employee for the Controller Connected Experiences, and on the necessity to perform a contract for the mobile Office apps. As assessed in paragraphs 11.1 and 11.2 of this report, consent of employees is not a valid legal ground for either Microsoft or government, and Microsoft cannot base the processing on the necessity to perform a contract because Microsoft does not have a valid contract with the employee. The government organisations only have a legal ground for diagnostic data processing for purposes that are strictly necessary.

Due to the lack of technical controls, the chance of occurrence of the risk of loss of control and unauthorised (further) processing is 100%, while negative consequences for data subjects cannot be excluded. Therefore, the lack of technical controls results in a high data protection risk.

16.2.3 Unlawful collection and storage of sensitive data through Controller Connected Experiences

The results of the data subjects access requests show that Microsoft does not collect many diagnostic data about the use of Office Online, and no content data from the contents of files, e-mail or chats, nor any file or path names. That is why the data protection impact on government employees resulting from the processing of usage data of Office Online can be assessed as low. Although the risks for data subjects are higher when Microsoft does process content data, such as file and path names stored in the log files about the use of SharePoint Online and OneDrive for Business, and the contents of documents which are processed through the Processor

[157] Ibid.

Connected Experiences, the chance of occurrence of the risks of loss of control and unlawful (further) processing remains low, since Microsoft as a data processor has agreed with SLM Rijk to only process these personal data for the three authorised purposes.

However, these risk mitigating contractual measures do not apply to the diagnostic data from the Controller Connected Experiences. Since government organisations are unable to technically prevent employees from using the Controller Connected Experiences in Office Online and the mobile Office apps, there is a reasonable likelihood for the occurrence of harm. The processing of the contents of documents 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). Therefore this results in a medium to high data protection risk.

16.2.4 Lack of purpose limitation mobile Office apps and Controller Connected Experiences

The diagnostic data from the mobile Office apps contain metadata about the individual use of the services. The diagnostic data from the Controller Connected Experiences are likely to include content, such as the contents of resumes when using the LinkedIn Resume Assistant. Both types of data may contain sensitive or confidential data.

As a result of the negotiations with SLM 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. Microsoft is more transparent about its role as data controller for the Controller Connected Experiences, but there is no control for administrators to centrally prohibit users from using these services in Office Online and in the mobile Office apps.

Microsoft contractually permits itself to process the diagnostic data from the mobile Office apps and the Controller Connected Experiences for all 14 purposes of its general Privacy Statement, including use for advertising. The observed traffic from three of the iOS apps to marketing company Braze shows that the processing for advertising purposes and personalised recommendations is not only a theoretical possibility.

Since government organisations make their employees work with Microsoft Office 365, but are unable to centrally prohibit the use of the mobile Office apps, or to prevent employees from using the Controller Connected Experiences in Office Online and in the mobile Office apps, they are factually joint controllers with Microsoft. As there is no such joint controller agreement, there is real risk that data subjects do not know where and how they can access their data protection rights.

The chance that the data protection risks occur because of loss of control, loss of confidentiality, reidentification of pseudonymised data and unlawful further processing is more likely than not. This report shows that there is no legal ground for most of the purposes Microsoft has as data controller for the processing of diagnostic data. This risk does not only apply to the processing of the historical diagnostic data, but also to Microsoft's technical ability to dynamically add new events.

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, 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.

16.2.5 No audit rights mobile Office apps and Controller Connected Experiences

Since Microsoft qualifies itself as a data controller for the mobile Office apps, the effective audit rights that SLM Rijk has negotiated with Microsoft do not apply to the diagnostic data processing from these apps. Similarly, SLM Rijk does not yet have an effective right to inspect the diagnostic data collected through the Controller Connected Experiences and the mobile Office apps. There are no known audit reports published by Microsoft with regard to these data.

The government organisations have a similar lack of control of the third parties engaged by Microsoft for the processing of personal data from these controller based services. As described in paragraph 2.2 of this report, in its general Privacy Statement, Microsoft explains that it can share personal data with third parties, such as affiliates and vendors, but that those companies must abide by the Microsoft security and privacy requirements. However, the fact that Microsoft requires such third parties to abide by Microsofts rules does not mean Microsoft has a GDPR-compliant data processor agreement with those parties.

Microsoft also has a paragraph titled "Advertising" in its general Privacy Statement, but this paragraph does not contain information about compliance with GDPR requirements, nor a limitative list of third parties that can be involved in Microsofts data processing for advertising purposes.

Given the lack of effective audit rights, the lack of transparency about third-party advertising companies, the inability to inspect contracts with third parties such as Braze, and the lack of a technical possibility for government organisations to turn off the Controller Connected Experiences in Office Online and the mobile Office apps, the likelihood of occurrence of data protection risks is more likely than not, while negative consequences for data subjects caused by unauthorised further processing and reidentification of pseudonymised data cannot be excluded. This results in a high data protection risk.

16.2.6 Employee monitoring system: chilling effect employees

If the government organisations start to deploy Office 365, and they use Office Online in combination with the Connected Experiences and the cloud storage and email services as well as Windows 10 Enterprise, Microsoft will collect many data about the work behaviour and lifestyle of government employees via the diagnostic data. This includes information about the times they work with the software and services, and for example their frequency of email usage. Microsoft actively offers tools to administrators to make such insights available.

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.[158]

[158] Microsoft, MyAnalytics vs. Workplace Analytics, Delve, and the Microsoft Graph, URL: https://docs.microsoft.com/en-us/workplace-analytics/myanalytics/overview/privacy-

These tools enable the government organisations to use the diagnostic data for a personnel tracking system. Processing for such a purpose results in a loss of control and loss of the right to (some) privacy at work, and unlawful further processing if incorrect conclusions are drawn 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 to become a whistleblower or for example contact certain people. In view of the dependence of employees of the use of Microsoft products and services at work, they have no means to evade the monitoring of their behaviour. The consequences for data subjects can be severe, up until incorrect dismissal.

Since the contents of the diagnostic data about the use of Office Online and the mobile Office apps are relatively innocent, the impact for data subjects of unlawful processing of these personal data is relatively minor, and therefore, this results in a low data protection risk.

However, unlawful processing, or unauthorised reidentification of the pseudonymised diagnostic data from the Connected Experiences and the cloud services can have a much higher impact on data subjects. The chance that this occurs is remote, if government organisations follow the advice from this report to first conduct a DPIA before using these tools. The chance that Microsoft causes these risks is also remote, in view of the contractual improvements with regard to purpose limitation and the right and commitment to audit.

16.2.7 No choice amount of diagnostic data

In Office 365 ProPlus version 1904 and later, government organisations have the possibility to influence the collection of diagnostic data, by choosing the Required or Neither setting for the telemetry data. Government organisations may also decide to turn off some or all of the Connected Experiences. However, these controls do not exist for Office Online or (at the admin level) for the mobile Office apps.

The government organisations have little to no control over Microsoft's processing of diagnostic data through the online services and mobile apps, other than not using many services included in the Office 365 license. As soon as government employees start to use the mobile Office apps or the Controller Connected Experiences, the government organisations enable Microsoft to collect the diagnostic data, and become joint data controllers with Microsoft for this data processing. The fact that employees can opt-out from the default setting 'full diagnostics' to 'basic diagnostics' on some of the mobile apps, does not provide the desired control at the admin level, nor the required data minimisation to the level of 'Neither'.

However, Microsoft does not accept a role as joint controller, and the possible conclusion of a joint controller agreement as determined in Art. 26 of the GDPR would only offer a cosmetic solution for the fundamental lack of control of the government organisations. In order for the government organisations to gain control

---

guide#myanalytics-vs-workplace-analytics-delve-and-the-microsoft-graph See also: 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 .

a combination is required of contractual measures (Microsoft as a data processor for the mobile Office apps), and technical measures (a setting to choose the minimum necessary volume and nature of the diagnostic data, comparable to the telemetry settings in Windows 10 and Office 365 ProPlus).

Since the contents of the diagnostic data about the use of Office Online and the mobile Office apps are relatively innocent, the impact for data subjects of unlawful processing of these personal data is relatively minor, and therefore, this results in a low data protection risk.

This assessment does not apply to the secret traffic from at least three of the iOS apps to the US-based marketing company Braze, but this has already been assessed as a high data protection risk in paragraph 16.2.1 of this report.

Unlawful processing, or unauthorised reidentification of the pseudonymised diagnostic data from the Connected Experiences and the cloud services can have a much higher impact on data subjects, but the chance that this occurs is remote, in view of the contractual improvements with regard to purpose limitation. SLM Rijk should use the right to audit to verify if the collected log data are necessary for the three authorised purposes, and whether Microsoft does not process excessive data.

16.2.8 Long retention period

The retention periods for diagnostic data at Microsoft vary between 30 days and 18 months, but Microsoft does not provide a detailed overview. The lack of transparency entails the risk that data subjects cannot exercise their rights. Additionally, the long retention period of the data in itself poses a data protection risk.

Although Microsoft has published a table with retention periods of data from Office 365, this table is not complete. It describes how long Microsoft stores certain data after a customer has deleted the data (active deletion), or if a customer ends the subscription (passive deletion). The table indicates that diagnostic data are stored between 30 and 180 days. However, this table does not provide any information about system-generated logfiles, and does not mention the storage period of 18 months for diagnostic data in Cosmos. In another document, Microsoft explains that the system-generated log files are stored for 180 days by default.[159]

Microsoft has provided a statement to SLM Rijk explaining that there are two retention periods for diagnostic data from Office 365 ProPlus: short term storage for 30 days, and long term storage for 18 months in the central Cosmos database in the USA. Microsoft has explained why a period of 18 months is necessary. According to Microsoft the efficacy of fixes, changes, or updates in software and services manifests in the longer term, including year over year, and customers may wait a year or longer to deploy Microsoft updates.

There is no possibility for users to delete historical diagnostic data per device ID, which Microsoft has been offering for historical Windows 10 telemetry data since April 2018. The only way government administrators can delete historical Office diagnostic data is by deleting the user account in Active Directory and by creating a new account for that user.

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

The GDPR requires that organisations only store personal data as long as necessary, because of the heightened risks of unlawful processing, incorrect data and data breaches. In view of the limited amount of data as shown by the telemetry analysis and the DSR results, the contractually agreed upon purpose limitation, and the fact that no direct identifiers nor content from documents in the diagnostic data were observed, the risks of unlawful processing or reidentification of pseudonymised historical data are remote, while the impact is also low. Therefore, the long period of 18 months for the diagnostic data does not lead to a high data protection risk.

This analysis of a low risk does not apply to the diagnostic data collected through the Controller Connected Experiences, or to the traffic sent from the mobile Office apps to the marketing company Braze. As analysed in paragraph 16.2.2 the inability for admins to technically prohibit the use of the Controller Connected Experiences, and the inability to prevent the download of the mobile Office apps leads to high risks for data subjects.

16.2.9 Transfer of personal data outside of the EEA

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.[160]

As has been explained in paragraph 12, there are risks related to 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 sub processors, 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. Therefore, there is a non-negligible risk that information held by Microsoft in a data centre in a third country can be accessed by local governments, through a hack or by forcing an administrator to do so.

With regard to the risk of hacks through rogue administrators or hostile state actors, on-premise local hosting does not offer better guarantees for a timely detection of new risks, and 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 technical and organisational measures that are regularly audited.

As explained in paragraph 7 of this report, Microsoft transfers the diagnostic data from Office Online and the cloud storage services to the United States as data processor with the EU Standard Contractual Clauses. Personal diagnostic data from the Controller Connected Experiences and the mobile Office apps are transferred under the terms of the EU-US Privacy Shield Framework. Microsoft has self-certified under this regime.[161] Although both of these transfer mechanisms are legally valid, and approved by the European Commission, there is serious doubt about the future validity of these instruments with regard to transfers to the USA. The European Court of Justice has been asked to decide whether this agreement and these clauses offer sufficient mitigation for the risks of extensive surveillance in the USA as

[160] The GDPR applies in the European Economic Area. This includes the member states of the EU and Iceland, Liechtenstein and Norway.
[161] Microsoft is an active participant in the Privacy Shield Framework https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK&status=Active

brought to light by whistle blower Edward Snowden, including the risk of data being observed in transit to the USA.[162]
These risks (of access to personal data by law enforcement authorities and security agencies in the USA) apply equally to the content data stored on Microsoft's cloud servers as well as to the diagnostic data, and they apply worldwide. Even though Microsoft provides guarantees with regard to storage of content data in datacentres in the Netherlands and Ireland, USA courts reserve the right to request access to these data under the USA CLOUD Act. This act essentially extends jurisdiction of the US-American courts to all data held by American corporations, even when that data is stored in data centres outside of the territory of the United States.

As explained in paragraph 5.2 of this report, Microsoft bi-annually publishes a transparency report about the amount of law enforcement requests it has received. Microsoft explains that very few law enforcement requests relate to Enterprise cloud customers.[163] According to the OST, Microsoft will in principle always inform the data controllers if the company receives such a request. Microsoft has explained that there is a very high legal bar for blind requests in the Enterprise environment (where Microsoft would get a nondisclosure order).

In the OST, Microsoft says: "*Microsoft will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.*"[164]

[162] In case 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. The court hearing took place on 9 July 2019. Advocate General Henrik Saugmandsgaard Øe will publish his Opinion on 12 December 2019. See for example: IAPP, CJEU's hearing on Schrems II has both sides worried ruling could be sweeping, 9 July 2019, URL: https://iapp.org/news/a/cjeus-hearing-on-schrems-ii-has-both-sides-worried-ruling-could-be-sweeping/ For Dutch speaking people, the ministry of Foreign Affairs publishes an overview of the different steps in this procedure at https://ecer.minbuza.nl/ecer/hof-van-justitie/nieuwe-hofzaken-inclusief-verwijzingsuitspraak/2018/c-zaaknummers/c-311-18-facebook-ireland.html. 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.
[163] Microsoft writes in its transparency report about law enforcement requests, in answer to a question about the number of requests for data from Enterprise customers: "*In the second half of 2018, **Microsoft received 61 requests from law enforcement around the world for accounts associated with enterprise cloud customers. In 39 cases, these requests were rejected, withdrawn, or law enforcement was successfully redirected to the customer.** In 22 cases, Microsoft was compelled to provide responsive information: 15 of these cases required the disclosure of some customer content and in 7 of the cases we were compelled to disclose non-content information only. Of the 15 instances that required disclosure of content data, 8 of those requests were associated with U.S. law enforcement.*" In answer to question about the effects of the CLOUD Act Microsoft writes: "*In the second half of 2018, Microsoft received 4,369 legal demands for consumer data from law enforcement in the United States. Of those, **103 warrants sought content data which was stored outside of the United States.** In the same time frame, **Microsoft received 36 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 that was stored outside of the United States**.*" Microsoft, Law Enforcement Requests Report, URL: https://www.microsoft.com/en-us/corporate-responsibility/lerr/.
[164] Microsoft OST, June 2019.

Although Microsoft also publishes bi-annual reports about orders from the security agencies, through FISA-orders, these reports only provide total aggregate estimates, not split per country or per type of customer (consumer or Enterprise).[165]

Outside of the Customer Data, the system-generated diagnostic data may also contain content data, special categories of data, and/or secret, classified and sensitive personal data related to the use of Connected Experiences and in file and path names stored in system generated log files from access to SharePoint Online and OneDrive for Business. These diagnostic data are stored in the USA, with the same risks to consider as described above.

Additionally, Microsofts guarantees to redirect law enforcement requests to customers do not apply to the diagnostic data from the mobile Office apps and the Controller Connected Experiences. The technical analysis of the telemetry data from the mobile Office apps and the results of the Data Subject Access Request for the diagnostic data from Office Online show that Microsoft collects a limited amount of information which do not include snippets of content or direct identifiers. However, because Microsoft qualifies itself as data controller for these personal data, the company makes no commitments to redirect law enforcement requests to the customer. In its general Privacy Statement, Microsoft only writes that it will disclose personal data, including content "*when we have a good faith belief that doing so is necessary to do (…) Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies.*"[166]

The risks from the transfer of diagnostic data to a provider outside of the EEA are not Microsoft-specific, but apply to all providers of cloud services. All cloud providers necessarily collect information about users' interaction with their servers (functional data), and store some of these data as diagnostic data. Microsoft and the government organisations cannot take any more measures to fully exclude occurrence of this risk.

As concluded by the European Data Protection Board and the EDPS in their recent advice to the LIBE Committee of the European Parliament about the CLOUD Act, transfers of personal data have to comply with Articles 6 (legal grounds) and 49 (exceptions to allow for transfer). In case of an order based on the US CLOUD Act, the transfer can only be valid if recognised by an international agreement. The data protection authorities emphasize the need for new MLATs and the need to successfully negotiate an international agreement 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 Standard Contractual Clauses for transfer of data from the EEA to the USA, and up to the European Commission to negotiate a new MLAT with the USA and a treaty about access for law enforcement.

Individual government organisations must assess the likelihood of the occurrence of one or all of the five general data protection risks identified in paragraph 16.2 of this report, in relation to the use of a cloud provider and the transfer of diagnostic personal data to the USA. Depending on their individual risk assessment, they can

[165] Microsoft, U.S. National Security Orders Report, URL: https://www.microsoft.com/en-us/corporate-responsibility/fisa . For example, in the first half of 2018, Microsoft received between 0 – 499 orders for content, relating to 13,000 - 13,499 accounts.

[166] Microsoft general Privacy Statement, last updated June 2019.

decide not to use any of the cloud storage services and/or work with strictly local accounts.

Although this DPIA only assesses the risks of the diagnostic data processing, government organisations should carefully assess the benefits of using additional encryption to add an extra layer of protection to the content data they store on Microsoft's cloud computers. 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 authorized 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.

Overall with regard to the mobile Office apps, Office Online and the Controller Connected Experiences the likelihood of the occurrence of unlawful access by courts or authorities in the USA is remote, while the impact on data subjects varies from minimal to 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 transparency: inability to exercise data subject rights and unlawful (further) processing
2. No technical opt-out for Controller Connected Experiences and mobile Office apps: loss of control, unlawful (further) processing
3. Unlawful collection and storage of sensitive data through Controller Connected Experiences: loss of confidentiality, inability to exercise data subject rights, loss of control
4. Lack of purpose limitation Controller Connected Experiences and mobile Office apps: unlawful further processing, reidentification of pseudonymised data
5. No audit rights SLM Rijk for Controller Connected Experiences and mobile Office apps: loss of control
6. No control over volume and nature of diagnostic data: loss of control
7. Chilling effects personnel monitoring system: inability to exercise related rights, such as the right to send and receive information
8. Long retention period: increased risk of reidentification of pseudonymised data and unlawful (further) processing
9. Transfer of limited diagnostic data to 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:[167]

Severity of impact	Serious harm	Low risk 9	High risk 3	High risk 1a, 1b

[167] 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/

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

Part D. Description of risk mitigating measures

Following the Dutch government's DPIA model, Part D describes the proposed counter-measures against the high data protections risks identified in part C.

Microsoft and the Dutch government have managed, through a combination of technical, legal and organisational measures, to mitigate the eight high data protection risks that were found in the first DPIA on the diagnostic data processing in Office 365 ProPlus. However, these risk mitigating measures do not apply to the diagnostic data processing through the mobile Office apps, and the data processing through the Controller Connected Experiences. This leads to five high and four low data protection risks.

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

17.1 Measures to be taken by Microsoft to mitigate high risks

No.	High risk	Measures to be taken by Microsoft
1	Lack of transparency	Public documentation about diagnostic data mobile apps and Controller Connected Experiences
		Enable data viewer tool for the mobile apps
		Enable data subjects to exercise their rights regarding Controller Connected Experiences and mobile Office apps
2	No technical opt-out Controller Connected Experiences and mobile Office apps	Temporary solution: technically prevent data subjects from using the mobile Office apps or do not ask for the consent (and do not process).
		Permanent solution: become a data processor for the mobile Office apps

		Create a central opt-out for data controllers to prevent use of the Contr. Connected Experiences via Office Online and the apps.
3	Unlawful collection and storage of sensitive categories of data through Controller Connected Experiences	Become a data processor for the mobile apps + central opt-out for Contr. Connected Experiences + exclusion of processing for the purposes of profiling, data analytics, market research, or advertising
4	Lack of purpose limitation mobile Office apps and Contr. Connected Experiences	Become a data processor for the mobile apps + exclusion of processing for the purposes of profiling, data analytics, market research, or advertising
5	Not enough control over sub-processors and factual processing	Ensure effective audit rights for the Dutch government regarding mobile Office apps and Controller Connected Experiences

In order to mitigate the remaining five high data protection risks, Microsoft should take the following measures:

1. Publish centrally organised, easily accessible, and detailed documentation about the diagnostic data collected via the Controller Connected Experiences and the mobile Office apps.
2. Modify the Data Viewer Tool to also show the telemetry events from the mobile Office apps.
3. Ensure that data subjects can effectively exercise their right to access personal data about their use of the mobile Office apps and the Controller Connected Experiences.
4. As a temporary solution: create an option for controllers to prevent data subjects from connecting in the mobile Office apps to their Enterprise work account, even if that organisation does not work exclusively with managed devices, or no longer ask for the consent of employees to process personal data through the Controller Connected Experiences (and stop storing any diagnostic data).
5. Allow administrators to technically opt-out from the use of the Controller Connected Experiences through Office Online and the mobile Office apps.
6. As a permanent solution: become a data processor for the mobile Office apps in the Enterprise environment. Apply all the legal guarantees to the mobile Office apps as negotiated by SLM Rijk for the online services and Office 365 ProPlus, including (1) the limitation to the three authorised purposes (2) the explicit prohibition to use the diagnostic data for marketing and advertising purposes and (3) granting effective audit rights.

17.2 Measures to be taken by government organisations to mitigate high risks

government organisations can take very few effective measures to mitigate these five high data protection risks.

1. Establish a policy to warn employees not to use the mobile Office apps and the Controller Connected Experiences
2. Inform employees about their access rights with regard to diagnostic data collected by Microsoft via DSR and the audit logs
3. As soon as technically possible: turn off the Controller Connected Experiences

17.3 Measures to be taken by Microsoft to mitigate low risks

No.	Low risk	Measures to be taken by Microsoft
6	No control over volume and nature diagnostic data	Offer technical data minimisations choices for telemetry and diagnostic data in all Office 365 services
7	Chilling effects perso monitoring system	Data minimisation, privacy by default settings
8	Long retention period of diagnostic data	Become a data processor for the mobile apps + central opt-out Contr. Connected Experiences
		Provide documentation about the different retention periods of all diagnostic data
9	Transfer of (limited amount diagnostic data to the USA	Data minimisation + become a data processor + effective audit rights. See par 7 and 16.8.2 for measures that should be taken by the European legislator

In order to mitigate the four low data protection risks, Microsoft should take the following additional measures:

1. Offer technical choices for administrators to minimise the diagnostic data collection in the mobile Office apps, Office Online and the cloud storage and email services.
2. Provide centrally organised, detailed, consistent, easily accessible and understandable documentation about the different retention periods of the diagnostic data from the mobile Office apps, Office Online, the Connected Experiences, and the cloud storage and email services.
3. Ensure that default settings influencing the collection of diagnostic data are set to privacy friendly.

17.4 Measures to be taken by government organisations to mitigate low risks

In order to mitigate the four low data protection risks, the government organisations should take the following additional measures:

1. Update the existing employee Privacy Statement with specific information for what purposes, and under what circumstances, the organisation may access the different diagnostic data from Microsoft's different services and products
2. Perform DPIAs before using analytical services based on the diagnostic data
3. As soon as technically possible: select the lowest, minimum level for the collection of diagnostic data
4. Support SLM Rijk in assessing the validity of transfer mechanisms after 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.

17.5 Measures EU legislator and EU 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 the transfer of diagnostic data from the EU to the USA.

Conclusions

Currently, the processing of diagnostic data about the use of the mobile Office apps and the Controller Connected Experiences leads to five high data protection risks. Only Microsoft can effectively mitigate these risks. Government organisations are advised to create policies for their employees to not use Office Online and the mobile Office apps. SLM Rijk will continue its negotiations with Microsoft to ensure that Microsoft realises the negotiated improvements for all services included in the Office 365 license.