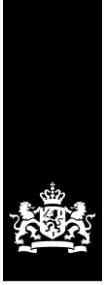


Ministerie van Justitie en Veiligheid

DPIA Office 365 ProPlus version 1905 (June 2019)
Data protection impact assessment on the processing of diagnostic data

Version 1

Date	22 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 ProPlus version 1905
Appendices	**1** Overview telemetry data observed at the levels 'required' and at level 'neither' **2** List of categories of data subjects and personal data
Authors	**Privacy Company** Sjoera Nas and Floor Terra, senior advisors www.privacycompany.eu

Contents

Summary

In May 2019, the Dutch government has commissioned a new Data Protection Impact Assessment (DPIA) on the processing of data about the use of the Microsoft Office 365 ProPlus software. This DPIA assesses the progress with commitments made by Microsoft after the first DPIA, published in November 2018. This report provides a technical analysis of the data about the usage of the new Office 365 ProPlus software version 1905 released by Microsoft on 11 June 2019. In a separate DPIA simultaneously published with this report, the risks are analysed of the use of Office Online and the mobile Office apps.

Results: No more high data protection risks
The outcome of this DPIA on Office 365 ProPlus is that Microsoft and the Dutch government have managed, through a combination of technical, contractual and organisational measures, to mitigate the eight high data protection risks from the first DPIA. These high risks were mostly due to a lack of transparency, a lack of purpose limitation and legal ground, lack of clarity about the role of Microsoft as data processor or as data controller, and the transfer of usage data, including contents of documents, to the United States while there was a lack of effective control mechanisms. If the administrators of Office 365 ProPlus follow the advice from this DPIA and, amongst others, set the telemetry to Neither and turn off the Controller Connected Experiences, there are no more known high data protection risks for data subjects related to the collection of data about the use of Microsoft Office 365 ProPlus.

Use by 300.000 government employees
The Office software is deployed on a large scale by different governmental organisations, such as ministries, the judiciary, the police and the taxing authority. Approximately 300.000 government employees work with the software on a daily basis, to send and receive e-mails, create documents and spreadsheets and prepare visual presentations. Generally, these organisations store the content they produce with the Office software in governmental data centres, *on premise*. Since the Dutch government currently tests the use of the online SharePoint and OneDrive for Business cloud storage facilities, this DPIA also includes the use of these cloud storage services. This DPIA also includes the use of the so called *Connected Experiences*. Those are online services that are closely integrated with the Office software, such as the spelling checker (Editor), the translator module and the possibility to include pictures from the internet.

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 Corporation in the USA. 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 functional data
This report addresses the data protection risks of the storing by Microsoft of data about the individual use of the Office 365 ProPlus software, including 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 Office telemetry client. Similar to the telemetry client in Windows 10, Microsoft has programmed the Office software to 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 and organisational measures to mitigate risks
In little over six months Microsoft has implemented important technical and organisational measures to mitigate or lower the data protection risks found for Office 365 ProPlus in the first DPIA.

Since May 2019, Microsoft has published extensive documentation about the Office ProPlus telemetry data. Microsoft has also modified the data viewer tool for Windows 10 telemetry events to also show the Office 365 ProPlus telemetry events. This allows data subjects to see the decoded Office ProPlus telemetry data Microsoft collects.

Since May 2019, Microsoft offers the most widely used and indispensable Connected Experiences such as the Editor (spelling checker), Translator and Office Help from a role as data processor, in stead of as data controller. There are 14 remaining Controller Connected Experiences. Microsoft allows administrators of Office ProPlus to centrally turn off these Controller Connected Experiences. This prevents the risk that employees are shown a question to provide consent for these services, while consent is not a valid legal ground for this data processing.

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

Since version 1904, released 29 April 2019, Microsoft also offers choices for administrators to minimise the amount of diagnostic data. Microsoft provides three options: Required, Optional and Neither.

The technical analysis of the diagnostic data collected at the levels of Required and Neither shows that the data do not contain any content from documents, emails or conversations, and no directly identifying data such as user names or e-mail addresses. The events related to the use of the processor Connected Experiences such as the spelling checker and Translator also do not contain snippets of content.

At the level 'Neither' Microsoft collects similar types of data as at the Required level, in spite of the claim that no diagnostic data about Office client software running on the user's device is sent to Microsoft. Some of the events at the 'Required' level contain more sensitive information, such as the exact number of pages, paragraphs,

lines, words, characters, spaces, pictures and citations in a Word document, as well as the interaction time in milliseconds that the data subject was actively interacting with the document.

In response to these findings, Microsoft has explained that there are two kinds of diagnostic data that are always collected and are not influenced by the new diagnostic data choice: required service data about the use of the Connected Experiences and diagnostic data about Essential Services such as authentication, telemetry and license checks. Both categories are also shown in the Data Viewer Tool.

Contractual improvements to mitigate risks
Microsoft has included a number of contractual privacy guarantees in the enrolment contract with the Dutch government. These guarantees ensure purpose limitation and the possibility for the Dutch government to verify compliance through effective audit rights. Microsoft has also contractually committed to its new role as data processor for most of the Connected Experiences.

As a data processor for the processing of usage data about Office 365 ProPlus, most of the Connected Experiences and cloud storage services, 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-data and (3) secure.

This strict purpose limitation applies to both the content (Customer Data) and to all diagnostic data, including the system-generated server logs. Microsoft has additionally guaranteed that it won't use the content data or the diagnostic data 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 on the use of diagnostic data to show 'tips' or recommendations for the use of Microsoft software and products that the customer has not purchased or does not use.

The Dutch government has also obtained effective audit rights, and will have an independent auditor perform an annual audit to verify compliance with these measures. A summary of the findings will be published by SLM Rijk.

Overview of implemented measures to mitigate high risks

No	High Risk	Measures taken by Microsoft
1	Lack of transparency	Public documentation and data viewer tool
2	No possibility for administrators to influence the collection of telemetry data	Since Dec 2018: temporary settings to minimise the processing
		Since release of version 1904: admin choices for telemetry levels
3	Unlawful collection and storage of sensitive or classified categories of data through Connected Experiences and diagnostic data on cloud servers with for example filenames	Contractual purpose limitation: processing only for three purposes for which the government organisations have a legal ground
		Microsoft is a data processor for most Connected Experiences + central opt-out from Controller Connected Experiences
		Microsoft will not use content or diagnostic data for profiling, data analytics, market research or advertising
4	Incorrect qualification Microsoft as data processor	Contractual purpose limitation
		Microsoft is a data processor for most Connected Experiences + central opt-out

No	High Risk	Measures taken by Microsoft
5	Not enough control over sub-processors and factual processing	Effective audit rights for the Dutch government to have an annual audit performed + commitment to conduct audit and publish summary of findings
6	Lack of purpose limitation	Contractual purpose limitation
7	Employee monitoring system: chilling effect	-
8	Long retention period of diagnostic data	Microsoft is a data processor for most Connected Experiences + central opt-out
		Contractual purpose limitation
		Limitation of future telemetry through switch
9	Transfer of data to the USA	Limitation of telemetry through switch + effective audit rights + contractual purpose limitation. See the paragraphs 7 and 16.8.2 for measures that should be taken by the European Commission

Recommended measures for government organisations
To mitigate the remaining data protection risks, government organisations can also take some measures themselves.

The recommended measures are:

1. Centrally prohibit the use of the Controller Connected Experiences;
2. Upgrade to version 1905 or higher of Office 365 ProPlus and set the telemetry level to 'Neither'. At the level 'Required' Microsoft collects slightly more sensitive data: the organisation needs to ensure that this data processing does not lead to a chilling effect amongst employees;
3. Set the telemetry level in Windows 10 Enterprise to 'Security' (or block telemetry traffic) and do not allow users to synchronise activities via the Timeline functionality. At higher levels, Windows telemetry also collects information about the use of Office ProPlus applications;
4. Disable sending of data for Customer Experience Improvement Program
5. Turn off Linked-In integration with Microsoft employee work accounts;
6. Conduct a DPIA before using Workplace Analytics and Activity Reports in the Microsoft 365 admin center and before allowing employees to use MyAnalytics and Delve;
7. Depending on the sensitivity of the content data: consider using Customer Lockbox and Customer Key;
8. Warn employees not to use Office Online and the mobile Office apps that are included in the Office 365 license until the five high risks have been mitigated.

Conclusions

As described in the letter sent on 1 July 2019 by the minister of Justice and Security and the minister of Interior Affairs and Kingdom Relation to members of parliament[1], Microsoft and the Dutch government have managed, through a combination of technical, contractual and organisational measures, to mitigate the eight high data protection risks from the first DPIA. If the government administrators take the recommended measures in this DPIA, as a result of the contractual and technical improvements there are no more known high data protection risks for data subjects related to the collection of data about the use of Microsoft Office 365 ProPlus.

[1] URL: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019Z13829&did=2019D28465

Introduction

This report, commissioned by the Microsoft Strategic Vendor Management office (SLM Rijk[2]) of the Ministry of Justice and Security, is a second data protection impact assessment (DPIA) on the processing of personal data about the use of the Microsoft Office 365 ProPlus software. This version of the Office software is installed locally, on the device of the users, but is used in combination with online Office 365 services.

This DPIA assesses the progress with commitments made by Microsoft after the first DPIA, published in November 2018. This DPIA provides a technical analysis of the data about the usage of the new Office 365 ProPlus software, in version 1905 released by Microsoft on 11 June 2019. This DPIA also takes the results into account of two rounds of negotiations between Microsoft and the Dutch government about contractual and technical improvements.

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.[3]

Umbrella DPIA versus individual DPIAs
The Microsoft Office software is used by approximately 300.000 employees and workers in the Dutch ministries, parliament, the High Councils of state, the advisory commissions, the police, the fire department and the judiciary, as well as the independent administrative authorities.[4] The Microsoft Office software is not new.

[2] SLM is the abbreviation of the Dutch words Strategisch Leveranciersmanagement Microsoft.
[3] *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017). For an explanation and examples (in Dutch) see: https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia.
[4] Source: Microsoft Business and Services Agreement, Amendment ID CTM, May 2017, last amended 10 May 2019.

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.[5]

In GDPR terms SLM Rijk **is not responsible** for the processing of diagnostic data through 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 365 ProPlus, SLM Rijk also publishes a DPIA on the risks of the processing of diagnostic data through Office Online and the mobile Office apps.

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.

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

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

[6] 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.

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 ProPlus, 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]

Scope: Office ProPlus with telemetry 'Required' and 'Neither'
Microsoft offers three telemetry settings for administrators in the new Office 365 ProPlus versions 1904 and up, released since 29 April 2019: Optional, Required and Neither. This report describes the differences in data protection risks for data subjects between the lowest levels of telemetry settings: Required and Neither. In this second scenario telemetry is still being collected on the device and sent to Microsoft. The events observed with the data viewer were largely the same as the events observed at the Required level, but some events were added and some events excluded.

This DPIA assesses the risks of data processing about the use of the five core apps (Word, Excel, Outlook, PowerPoint and Teams) in combination with the Connected Experiences (such as the spelling checker) and use of the Microsoft cloud storage services SharePoint Online and OneDrive, a so called *hybrid* set-up.

The risks of data processing at the Optional level of telemetry are **outside the scope** of this DPIA. Additionally, this DPIA does not assess the data protection risks of the use of Office 2019, Office Online or the mobile Office apps, or other software that is included within the government Office 365 licenses.

The exact scope is detailed in paragraph A1.3 of this report.

Technical analysis of the telemetry data
This report provides an analysis of the contents of the telemetry data as collected by the test lab created by SSC-I for the Ministry of Justice and Security in June 2019.

The lab has performed a number of scripted scenario's on Virtual Machines with Windows 10 Enterprise 1809 and Office 365 ProPlus version 1905 (Build 11629.20246).[9]

In close dialogue with Privacy Company, the technical lab has performed scripted scenario's on virtual machines. The scenarios were drafted to capture data from common use by government employees, but they are limited in time and scope. The scenarios involved the execution of a scripted actions in each of the five most widely

[7] Ibid.
[8] https://www.privacycompany.eu/
[9] The lab experienced problems testing version 1904, because of the combination of English group policies while Dutch was set as the language for the OS and applications. See the Microsoft Office update history at https://docs.microsoft.com/en-us/officeupdates/update-history-office365-proplus-by-date (last visited and recorded on 8 July 2019).

used Office tools (Word, Excel, PowerPoint, Outlook and Teams). These actions were activities such as opening and storing a document, sending an e-mail, including a picture in a PowerPoint, and misspelling a few words in Word. In each of those apps, several Connected Experiences were used, and documents were stored and retrieved from SharePoint Online and OneDrive for Business.

The scenarios represent the collection of diagnostic data with the telemetry set to Required and to 'Neither', with the Windows 10 telemetry level set to the lowest level of Security.

The technical lab relied on the newly expanded functionality of Microsoft's Diagnostic Data Viewer to detect and record the outgoing telemetry. As an essential security measure, Microsoft encodes the outgoing traffic to its own servers in a way that makes inspection of the content of the traffic impossible with normal proxy-techniques. The technical lab also recorded all outgoing network traffic with Network Monitor and Fiddler. This setup ensures that any unexpected network traffic would be noticed. All the captured outgoing telemetry and traffic has been stored and provided in csv format to Privacy Company. Additionally, the lab has recorded all settings and actions on virtual disk images and has stored these images to be able to reproduce all actions and resulting telemetry events.

The analysis of the collected telemetry data in this report is a snapshot, because Microsofts collection of telemetry data is dynamic. Microsoft can add telemetry events on the fly, and collect other types of data, if it assesses that the purposes comply with the purposes described in this report.

The details of the executed scenario's and main findings from the technical investigation are described in part A of this DPIA. Privacy Company has compared the results with the publicly available documentation from Microsoft about the Office telemetry data. In this documentation, Microsoft sometimes uses the word 'obsolete' for telemetry events that may still be collected, but has been or will soon be removed from the diagnostic data at the Required level.

Response Microsoft
SLM Rijk has asked Microsoft to comment on the technical findings with regard to the telemetry settings of 'Neither' and 'Required', and to provide information on the default setting (for admins) of sending data to Microsoft for the Customer Experience Improvement Program (CEIP). Microsoft has replied by e-mail of 19 July 2019. The specific answers are included in paragraphs 2.1.1 (Technical analysis telemetry data) and 3.2 (Privacy Choices in Office 365 ProPlus).

Outline
This assessment follows the structure of the *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017).[10] 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

Part A explains the Office service in detail. This starts with a description of the technical way the data are collected, and describes the categories of personal data

[10] 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

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 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 (remaining) risks for data subjects are assessed, as caused by the processing activities related to the collection of usage data of Office ProPlus.

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

Part A. Description of the Office diagnostic data processing

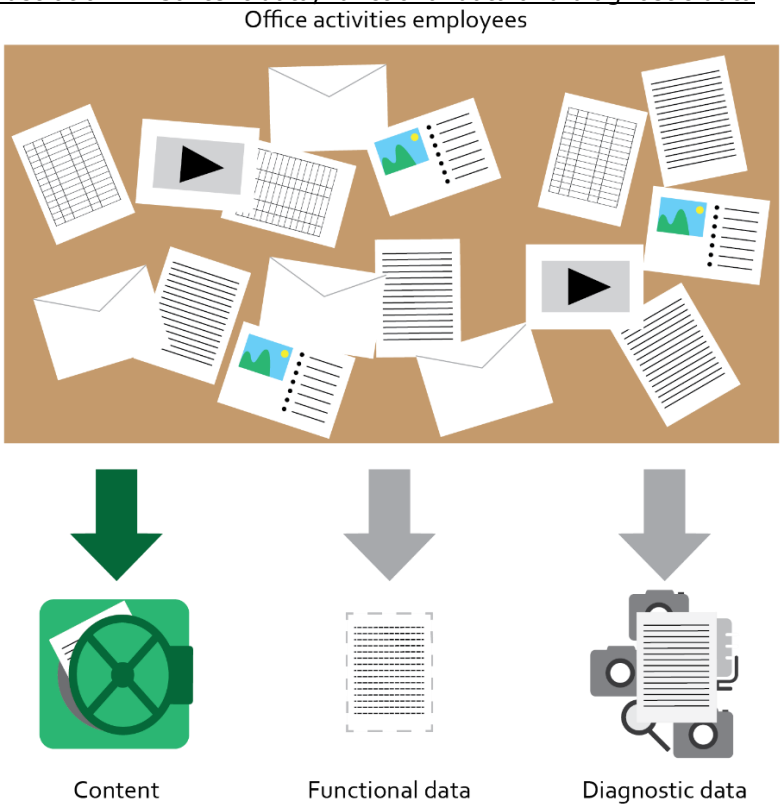
This first part of the DPIA provides a description of the characteristics of the diagnostic data collected via the use of Office 365 ProPlus software. This starts with a short description of the processing of different kinds of data (content, diagnostic data and functional data).

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 and Microsoft as processor and (sometimes) 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 the Microsoft Office 365 ProPlus software (not Office ProPlus 2016 or 2019), 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



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 Microsofts 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 Microsofts 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. (…)*"[11] 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 the Processor Connected Experiences such as the Editor (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.[12] 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.

Microsoft uses different words and classifications. The term 'diagnostic data' for Microsoft refers to the specific telemetry data collected through Office 365 ProPlus about the use of the Office software. Microsoft does not have an overall category for

[11] 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*

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

the 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.[13]

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 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 365 ProPlus and 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 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 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'.[14] 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. 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 allows itself to process the resulting personal data for its own purposes, as outlined in its General Privacy Statement.

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

[13] Slides presented by Microsoft on 1 November 2018.
[14] 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).

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*.

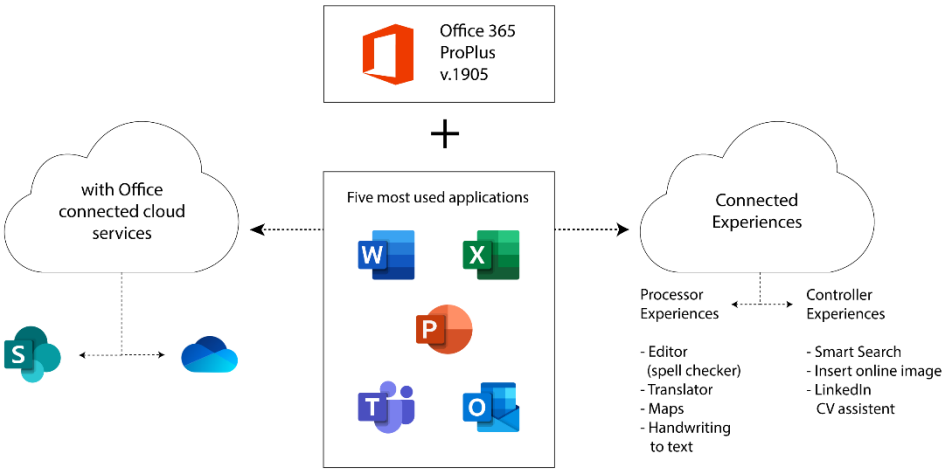
1.2 Scope

The aim of this DPIA is to assess whether and how the new Office 365 ProPlus software can be deployed in a GDPR compliant manner by the government organisations in relation to the processing of data about the usage of the software. This DPIA analyses the collected telemetry data at the two lowest levels of telemetry: 'Required' and 'Neither'.

This report specifically assesses the mitigating measures implemented by Microsoft to ensure that the processing of personal data related to the use of the Office services 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.

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

Illustration 2: Assessed Office 365 services and applications



This report also contains a few references to technical research conducted by Privacy Company early in 2019 related to the telemetry data collected, amongst others, through Connected Experiences: the LinkedIn CV assistant and Insert Picture. These telemetry events were captured in the network traffic by the technical lab, while it was executing the scripted scenarios for the first Office 365 ProPlus DPIA report. Privacy Company was able to decode relevant parts of the contents of the collected telemetry data. Since these diagnostic data were generated in a previous version

1708 of Office 365 ProPlus, these events allow for a check on the improvements Microsoft has implemented.[15]

Out of scope
This DPIA is limited to the diagnostic data processing from Office 365 ProPlus. Microsoft has not made similar improvements for Office 2016 ProPlus and Office 2019 ProPlus. This DPIA report does not provide an analysis of the data protection risks caused by the use of Office Online (Microsoft cloud based apps accessed through a browser) or the mobile Office apps that can be installed on mobile devices with iOS and Android operating systems. Those two versions of Office are the subject of a separate DPIA that is published simultaneously with this DPIA by SLM Rijk.

This report describes the storage and retrieval of documents in SharePoint Online and OneDrive for Business, 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 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 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.

This DPIA does not assess the risks of using Office 365 ProPlus on Macs. Though Microsoft has announced some improvements for the Office for Mac and for the mobile Office apps, it is not clear what these improvements are, and what they entail.

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.*"[16]

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.

Given the short timeframe to conduct this DPIA, other choices had to be made about the scope. This DPIA discusses the separate tools Activity Reports in the Microsoft 365 admin center, Workplace Analytics, Delve and MyAnalytics as examples of the use of diagnostic data, but does not present a full risk analysis. The outcome of this

[15] In the initial Office 365 ProPlus DPIA report the following to versions were tested: Microsoft Office Professional Plus 2016 MST 1806 (build 10228.20080 Click to run) and Microsoft Office 365 (Subscription Microsoft Office 365 ProPlus – Semi Annual Channel o version 1708 (Build 8431.2270 Click to run).
[16] 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).

brief examination is that government organisations need to perform a DPIA before they use the service themselves (Activity Reports in the Microsoft 365 admin center and WorkPlace Analytics) or allow employees to use these analytical services (Delve and MyAnalytics).

This DPIA mentions the combination of Office diagnostic data with LinkedIn diagnostic data (through the Controller Connected Experience LinkedIn CV assistant), but does not provide a full overview of the risks of all Controller Connected Experiences.

Last but not least, 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.

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 1 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 the Office applications, 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, in relation to the documentation newly published by Microsoft. This paragraph ends with a description of the contractual guarantee provided to Microsoft in relation to the process of anonymisation.

2.1 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 the previous Office ProPlus DPIA report extensive legal, technical and organisational arguments were provided why the diagnostic data were personal data as defined in Art. 4(1) of the GDPR.[17]. Microsoft has since confirmed that the different

[17] Art. 4(1) of the GDPR: ***'personal data'*** *means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to*

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.[18]

To just repeat briefly:

- Legal: The Dutch DPA concluded in its public investigation report about Windows 10 telemetry data in 2017 that Windows 10 telemetry data are personal data. During this investigation Microsoft claimed that most Windows 10 telemetry data did not relate to natural persons, but only to (technical aspects of) the operating system. The Dutch DPA explained that when object data are combined with other data, the resulting data set may contain information relating to an individual. The Dutch DPA established, with the help of the Windows data viewer tool, that all event data contained one or more identifiers that could be related to identifiable persons.

- Organisational: the reasonable assumption of Microsofts' capability as a technology provider to be able to combine different telemetry events over time to identify a single user. Additionally, as part of its research, the Dutch DPA filed a data subject access request for its research accounts and established that it was factually possible for Microsoft to link the e-mail addresses to the user identifiers, and the user identifiers to device identifiers.[19]

- Practical: the examples in the first DPIA report from the audits log about the use of the Office ProPlus software in the tested scenarios. According to Microsoft, the audit logs provide detailed information about product and service usage data contained in system-generated logs, such as the logs created by the use of the Connected Experiences, Exchange Online, SharePoint Online en OneDrive for Business.[20] Microsoft has explained that the company will include data from server generated system logs in the output of a Data Subject Request if they are personal data.[21]

- Contractual: In its Online Service Terms, Microsoft acknowledges: "*Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Online Service is also Customer Data.*"[22] This includes content data that Microsoft may collect through the Online Experiences. Microsoft has explained that if a user utilises a Connected Service for which Microsoft considers itself to be a data processor, that the content uploaded by the user is Customer Data, and will be treated as personal data.

---

the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

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

[19] Ibid, p. 103.

[20] 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.*"

[21] See footnote 6, first Office ProPlus DPIA report, 7 November 2018, with reference to Meeting report 28 August 2018, answer to Q2.

[22] Microsoft OST July 2019, p. 8: Processing of Personal Data: GDPR:

2.1.1 *Technical analysis telemetry data*

Technically, Microsoft Corporation collects diagnostic data about the use of Office 365 in different ways, via system-generated event logs on its own servers and via the Office telemetry client. Similar to the telemetry client in Windows 10, Microsoft has programmed the Office software to collect telemetry data on the device, and regularly send these to Microsoft

This DPIA report contains examples of collected telemetry events. They provide insight in the volume, nature and sensitivity of the data that Microsoft collects via the in-built telemetry client in Office 365 ProPlus. **Appendix 1** with this DPIA report contains an overview of all captured telemetry events in the two tested settings Required and Neither and the full contents of some selected events.

As explained in the introduction, the technical lab has not only captured telemetry data with the Data Viewer Tool, but has also recorded all outgoing traffic with Network Monitor and Fiddler. **In none of these data streams any events were observed that could be attributed to Teams.**[23]

The telemetry data shown in the Diagnostic Data Viewer about the use of the other four applications (Word, Outlook, PowerPoint and Excel) show that Microsoft collects several unique identifiers relating to the user, the device and the tenant. Microsoft collects limited information about tasks performed in the different applications and Connected Experiences. This includes information such as the size in bytes of document, the duration of the activity and the number of co-authors.

The observed telemetry data do not contain any content from documents, emails or conversations, and no directly identifying data such as user names or e-mail addresses. The events related to the use of the processor Connected Experiences such as the spelling checker and Translator also do not contain snippets of content.

This finding is in line with Microsofts explanation:

"*This diagnostic data doesn't include names of users, their email addresses, or the content of their Office files. Our system creates a unique ID that it associates with your user's diagnostic data. When we receive diagnostic data showing that one of our apps crashed 100 times, this unique ID lets us determine if it was a single user who crashed 100 times or if it was 100 different users who each crashed once. We don't use this unique ID to identify a specific user.*"[24]

In its response to the previous DPIA, Microsoft explicitly denied that customer content could be included in the diagnostic data. Microsoft wrote that the inclusion of content is explicitly prohibited by diagnostic data collection rules and is enforced by the product team's privacy personnel and privacy governance structure. In addition, Microsoft wrote it has automated checks and balances in the form of tools and processes to detect and correct issues if a bug results in this type of data being inadvertently collected.[25]

At both telemetry levels Microsoft does sometimes collect a hash of a file name from SharePoint Online or hashed URL of a location. The locations and URLs of files are data of a sensitive nature, as they may be confidential/ restricted/classified

[23] Remarkably, Microsoft collects a high amount of data with a very high frequency from the Teams app in iOS. See the DPIA report for SLM Rijk on Office Online and the mobile Office apps.
[24] Microsoft, Overview of privacy controls for Office 365 ProPlus, last updated 6 May 2019.
[25] E-mail Microsoft to SLM Rijk, 4 November 2018.

information, and/or contain directly identifying personal data. These personal data may have a sensitive nature. Employees habitually include their own names in document titles. The file paths may reveal sensitive or special categories of data, for example if an organisation that works with health data, has a document structure in which file paths may include names of diseases or medical expertise.

Microsoft explains the difference between the three telemetry levels as follows:

- ***If you choose Required**, the minimum data necessary to help keep Office secure, up-to-date, and performing as expected on the device it's installed on is sent to Microsoft.*
- ***If you choose Optional**, additional data that helps make product improvements and provides enhanced information to help detect, diagnose, and remediate issues is sent to Microsoft. If you choose to send optional diagnostic data, required diagnostic data is also included.*
- ***If you choose Neither**, no diagnostic data about Office client software running on the user's device is sent to Microsoft. This option, however, significantly limits Microsoft's ability to detect, diagnose, and remediate problems that your users may encounter when using Office.*[26]

Additionally, Microsoft explains:
"Required diagnostic data helps to identify problems with Office that may be related to a device or software configuration. For example, it can help determine if an Office feature crashes more frequently on a particular operating system version, with newly introduced features, or when certain Office features are disabled. Required diagnostic data helps us detect, diagnose, and fix these problems more quickly so the impact to users or organizations is reduced."[27]

Examples of optional diagnostic data include data we collect about the shapes users insert into Word documents so we can provide better options, and data we collect about the time it takes for a PowerPoint slide to appear on your screen so we can improve the experience if it's slow.[28]

Even though Microsoft provides extensive documentation about the Office ProPlus telemetry events since May 2019, this documentation is not complete nor clear. For 113 of the captured 226 different telemetry events no public documentation could be found (See **Annex 1** with this report).

There are two additional categories of telemetry data: required service data about the use of Connected Experiences, including the use of online cloud storage services, and diagnostic data about essential services. The collection of these data by Microsoft is not optional and cannot be turned off: the collection is not influenced by the telemetry settings.

Required service data
Required service data are related to the use of Connected Experiences. Microsoft explains: *"We give you the ability to choose which types of connected experiences you want to use in Office, which then determines what required service data is sent*

[26] Microsoft, Use policy settings to manage privacy controls for Office 365 ProPlus, 6 May 2019, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/manage-privacy-controls (URL last visited and recorded on 8 July 2019).
[27] Microsoft Required diagnostic data for Office, 10 June 2019.
[28] Microsoft, Optional diagnostic data for Office. 2 July 2019. URL: https://docs.microsoft.com/en-us/deployoffice/privacy/optional-diagnostic-data (URL last visited and recorded on 8 July 2019).

to us. PowerPoint Designer, for example, is one of several connected experiences that analyzes your content."[29]

Microsoft explains that these required service data from the Connected Experiences also appear in the Diagnostic Data Viewer. Microsoft only provides five examples of these required service data, namely:

- Office.Excel.Coauth.SaveXrr
- Office.Excel.Coauth.CloseWorkbook
- Office.Security.OCX.NonTrustedEncounter
- Office.Security.UrlReputation.GetUrlReputation
- Office.Voice.VoiceManager.StreamingAudio[30]

Microsoft writes: "*The events for service diagnostic data provide us necessary information about whether a connected experience is performing as a customer would expect. For example, whether the service used by the connected experience started successfully and was available when needed, whether there were errors or other unexpected issues (crashes) when interacting with the service, and the responsiveness or performance of the service.*"

Of the captured telemetry events mentioned in **Appendix 1** with this report 11 different events provide information about co-authoring activities in Excel and two events are about Security.UrlReputation. These 16 events therefore seem to be part of these required service diagnostic data.

But those are not the only required service data. Microsoft uses a very broad scope for Connected Experiences. Microsoft explains that "*Working with others on a document stored on OneDrive*"[31] is an example of a Connected Experience, just like Teams is. These Connected Experiences are not included in the four lists of Connected Experiences that Microsoft publishes:

1. Connected experiences that analyze your content
2. Connected experiences that download online content,
3. Other connected experiences
4. And, partially overlapping: optional Controller Connected Experiences

Microsoft apparently also includes all services that are related to the use of cloud storage and email services, and the use of Teams. In response to the observation that no telemetry data were observed from Teams, Microsoft has explained that Teams is a continually connected service, and therefore continually sends Required Service Data to Microsoft. These *required service data* include diagnostic data as well as other classes of data (functional data and content data).[32] Microsoft writes: "*The Diagnostic Data for both Office client software as well as Diagnostic data which is part of "Required service data" can be observed through the Diagnostic Data viewer.*"[33]

Microsoft has not responded to the observation that the data viewer tool did not show any events related to Teams.

Essential services

Microsoft explains that there is "*a set of services that are essential to how Office functions and therefore cannot be disabled. For example, the licensing service that*

[29] Microsoft, Required service data for Office, 6 May 2019, URL: https://docs.microsoft.com/en-gb/DeployOffice/privacy/required-service-data (URL last visited and recorded on 8 July 2019).
[30] Ibid.
[31] Microsoft, Connected Experiences in Office, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/connected-experiences.
[32] E-mail Microsoft to SLM Rijk 19 July 2019.
[33] Ibid.

confirms that you are properly licensed to use Office. Required service data about these services is collected and sent to Microsoft, regardless of any other privacy-related policy settings that you have configured. You can see this data by using the Diagnostic Data Viewer."[34]

The event *Office.Licensing.OfficeClientLicensing.DoLicenseValidation* was observed 124 times at the Required level, and 228 times at the Neither level. Microsoft explains the purpose of the category Licensing: *"a cloud-based service that supports your Office activation for new installations and maintains the license on your devices after Office has been activated. It registers each of your devices and activates Office, checks the status of your Office subscription, and manages your product keys."*[35]

Microsoft provides detailed documentation about the different telemetry events captured by these Essential Services. Microsoft mentions 6 broad categories of events that belong to these essential services. Besides Licensing, this also includes 'Authentication', 'Click-to-Run', 'Enhanced Configuration Service (ECS)', 'Telemetry' and 'Services Configuration'. The category Telemetry events contains events about SystemHealth and the functioning of the telemetry client and data viewer.

Telemetry set to Required
At the Required level of telemetry, Microsoft collects information that is common to all events. This information is collected in the following categories:

Categories and data fields that are common for all events
App
- *Name - The name of the application that is providing the data. Allows us to identify which application is showing an issue so we know how to address it.*
- *Platform - The broad classification of the platform on which the app is running. Allows us to identify on which platforms an issue may be occurring so that we can correctly prioritize the issue.*
- *Version - The version of the application. Allows us to identify which versions of the product are showing an issue so that we can correctly prioritize it.*

Client
Identifier related to an Office instance on a device. Constant for all sessions of all apps of a given installation version for multi-app suites, or constant for all sessions of a given application version. This category contains the following fields:

- *Id - Unique identifier assigned to a client at install time of Office. Allows us to identify whether issues are impacting a select set of installs and how many users are impacted.*

Consent
Information regarding the users consent for diagnostic data and connected experiences. (…)
Device / Legacy / Release
(…)
Session
(…)
User
- *PrimaryIdentityHash – A pseudonymous identifier that represents the current user.*
- *PrimaryIdentitySpace – The type of identity contained in the PrimaryIdentityHash. One of MASCID, OrgIdCID or UserObjectId.*

[34] Microsoft, Essential services for Office, 10 June 2019, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/essential-services
[35] Ibid.

• TenantGroup - The type of the tenant that the subscription belongs to. Allows us to classify issues and identify whether a problem is widespread or isolated to a set of users.
• TenantId - The tenant that a user's subscription is tied to. Allows us to classify issues and identify whether a problem is widespread or isolated to a set of users or a specific tenant.
Information that specifically supports diagnostic data collection
• AggMode - Tells the system how to aggregate activity results. Allows us to reduce the amount of information uploaded from a user's machine by aggregating activity results into a single event that gets sent periodically.
• Count - The number of times the activity happened if the count is from an aggregated event. Allows us to determine how often an activity succeeded or failed based on the aggregation mode of the activity.
• CV - A value that identifies the relationship between activities and sub-activities. Allows us to rebuild the relationship between nested activities.
• Duration - The length of time the activity took to execute. Allows us to identify performance issues that are negatively impacting the users experience.
• Result.Code - An application defined code to identify a given results. Allows us to determine more specific details of a given failure such as a failure code that can be used to classify and fix issues.
• Result.Tag - An integer tag that identifies the location in code where the result was generated. Allows us to distinctly identify the location in code where a result was generated which enables classification of failures.
• Result.Type - The type of the result code. Identifies what type of result code was sent so that the value can be correctly interpreted.
• Success - A flag indicating if the activity succeeded or failed. Allows us to determine if actions the user takes in the product are succeeding or failing. This allows us to identify issues that are impacting the user. [36]
[etcetera]

At the Required level of telemetry, at least one event contains very detailed statistics about a Word document and the time in milliseconds a user was actively working on it. The event *Office.Word.Experimentation.DocumentStatsOnCloseAnd Suspend* sends information to Microsoft with the exact number of pages, paragraphs, lines, words, characters, spaces, pictures and citations in a Word document, as well as the active interaction time in milliseconds. Microsoft explains in its public documentation about this event: "*This event logs document statistics for each document when Office Word is closed or suspended. The event is used to correlate document edits, size, etc. with document-save, document-share, and document-online-collaboration errors.*"[37]

Other events at the Required level collect information such as the number of special characters in a document or in the title/URL of a document, and detached duration as well as stopwatch duration of the total time of the activity.

For example with the event *Office.PowerPoint.DocOperation.SaveAs* Microsoft collects hashed information about the files and locations of files in SharePoint Online and OneDrive for Business, and about the type and duration of user activity in PowerPoint. According to Microsofts public explanation, this event contains 84 different fields. The

[36] Microsoft, Categories and data fields that are common for all events, 10 June 2019, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data#categories-and-data-fields-that-are-common-for-all-events (URL last visited and recorded on 8 July 2019).
[37] Microsoft, Required diagnostic data for Office, Product and service usage data events, 10 June 2019, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data#product-and-service-usage-data-events (URL last visited and recorded on 8 July 2019).

following 14 fields contain information about the size and location of source (SRC) and destination (DST) of files, number of co-authors and duration of user activity:

1. Data_DstDoc_FqdnHash:string - Hash of where document is stored
2. Data_DstDoc_ResourceIdHash:string - Hash of resource identifier for documents stored in cloud
3. Data_DstDoc_ServerDocId:string - immutable identifier for documents stored in cloud
4. Data_DstDoc_StorageProviderId:string - A string that identifies the document's storage provider, like "DropBox"
5. Data_SrcDoc_Fqdn:string - Where is document stored (SharePoint.com, live.net), only available for Office 365 domains
6. Data_SrcDoc_FqdnHash:string - Hash of where document is stored
7. Data_SrcDoc_LocationDetails:long - Predefined set of values of more detailed location (Temp folder, downloads folder, One Drive Documents, One Drive Pictures etc.)
8. Data_SrcDoc_NumberCoAuthors:long - Number of co-authors at the time of opening of a document
9. Data_SrcDoc_ResourceIdHash:string - Hash of resource identifier for documents stored in cloud
10. Data_SrcDoc_SizeInBytes:long - Document size in bytes
11. Data_SrcDoc_UrlHash:string - hash of full URL of documents stored in cloud
12. Data_StopwatchDuration:long - Total time for Activity
13. DstDoc - New location of document
14. SrcDoc - Original location of document[38]

Both these events are included with all fields in **Appendix 1** with this DPIA report.

Telemetry set to 'Neither'
The technical analysis of the telemetry data shows that Microsoft collects 173 different telemetry events at the level Neither, compared to the 166 different events collected at the level Required. 60 telemetry events occur only at the Neither level, while 53 other events from the Required level are excluded at the level Neither. In total, 226 different telemetry events were observed.

The captured events at the level 'Neither' are not empty, but contain information about activities performed in the four applications. These events also contain the unique identifiers and events which according to Microsoft occur in all events.

At the Neither level, Microsoft collects information about the location and size of files, number of co-authors and a count of the number of times a file was for example opened, in addition to the unique user and device ID's described above.

For example, the event *Office.FileIO.CSI.CcachedFileCsiLoadFileBasic* contains 116 different fields according to Microsoft. The following 15 fields contain information about the size and location of files, number of co-authors and incremental count the document was opened:

1. Data.Doc.Fqdn - OneDrive or SharePoint Online Domain Name
2. Data.Doc.FqdnHash - One-way hash of customer identifiable domain name
3. Data.Doc.Location - Indicates which service provided the document (OneDrive, File Server, SharePoint etc.)

[38] Ibid, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data#officepowerpointdocoperationsaveas (URL last visited and recorded on 8 July 2019).

4. Data.Doc.LocationDetails - Indicates which Known Folder provided a locally stored document
5. Data.Doc.NumberCoAuthors - Count of the number of fellow users in a collaborative editing session
6. Data.EditorsCount - A count of other collaborators editing the document
7. Data.Location - Indicates storage media type/location (USB, Cloud, etc.)
8. Data.Doc.ResourceIdHash - An anonymized document identifier used to diagnose problems
9. Data.Doc.ServerDocId - An immutable anonymized document identifier used to diagnose problems
10. Data.Doc.SessionId - Identifies a specific document edit session within the full session
11. Data.Doc.SizeInBytes - Indicator of document size
12. Data.Doc.UrlHash - One-way hash to create a naïve document identifier
13. Data.Doc.UsedWrsDataOnOpen - Diagnostic indicator for incremental document open
14. Data.ResourceIdHash - Obsolete
15. Data.StopwatchDuration - Obsolete[39]

When asked to respond to the finding that there seems to be little difference between the 'Neither' and 'Required' settings, Microsoft explained that there is a major difference, but that the amount of captured telemetry data perhaps stems from the two other categories of telemetry data that are shown in the Data Viewer Tool, the Required Service Data and the diagnostic data about Essential Services.

Microsoft writes: "*When "Neither" is chosen the Office 365 ProPlus client ceases to send diagnostic data about Office 365 ProPlus client, as documented. However, other diagnostic data, from connected services and other events as part of Connected Experiences, are unaffected by this setting and this may be what is confusing the analyst. For example, Required Service Data for any connected experience (whether a small one in Office 365 ProPlus or the entirety of an continually connected service like Teams) includes diagnostic data as well as other classes of data (functional data and content data). It is not diagnostic data about events in the client software but data about the usage of the connected service/experience.*"[40]

This statement from Microsoft explains why events such as storing and retrieving documents from the cloud storage services SharePoint Online and OneDrive for Business are shown by the Data Viewer Tool if the telemetry level is set to 'neither'. But absent meaningful and exhaustive documentation of the telemetry events captured by the Connected Experiences (Microsofts category of 'required service data'), this explanation does not fully cover the extent of telemetry data collected by Microsoft.

Comparison to diagnostic data in the previous Office 365 ProPlus version

Compared to the telemetry collected through the previous version 1708 of Office 365 ProPlus, at the new levels of Required and Neither, Microsoft has reduced or pseudonymised the contents of the collected telemetry data, as announced at the end of 2018. Microsoft had explained: "*The Diagnostic Data collection SDK does not provide for systematic commingling of Customer Data or Customer Data content being processed in an Office 365 Pro Plus application with Diagnostic Data from the same*

[39] Microsoft, Required diagnostic data for Office, 10 June 2019, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data#officefileiocsiccachedfilecsiloadfilebasic (URL last visited and recorded on 8 July 2019).
[40] E-mail Microsoft to SLM Rijk 19 July 2019.

application. Nor does Microsoft systemically or generally perform commingling of Online Services or Connected Services customer data content with Diagnostic Data. However the Diagnostic Data SDK does provide for generic fields [that] can be encoded to have meaning specific to the event. If Microsoft was to discover Customer Data content had been encoded into such fields then Microsoft would move fast to treat this as a critical bug and eliminate the encoding."[41]

In the previous Office 365 ProPlus version 1708, as decoded by Privacy Company, Microsoft collected file names as well as unhashed path names of documents. For example the event *Office.PowerPoint.DocOperation.SaveAs* revealed more information about the location of data. In the tested scenario a PowerPoint presentation was opened and stored on Microsofts cloud services SharePoint Online and OneDrive for Business. Via the events **Data.FilePath, Data.SaveFromLocation, zP.Data.SaveFromLocation, zP.Data.SaveTo Location** and **Data.SaveToLocation**, as well as the events **zP.Data.FileHash** and **zP.Data.FilePath** Microsoft collected information in clear text about the names of files and the pathnames stored in SharePoint Online and OneDrive for Business.

As explained above, file and path names may reveal confidential/restricted/classified or state-secret information and/or contain directly identifying personal data.

In the previous Office 365 ProPlus version 1708, as decoded by Privacy Company, Microsoft apparently also routinely matched contents of Word documents to infer if the document was a resume, to prepare for the use of the **LinkedIn Resume Assistant**. During the execution of the tested scenarios, Microsoft did not ask for consent to scan the document for this specific purpose. For example with the telemetry event *Office.Word.LinkedIn.NLGAugmentorResumeClassificationResult*.

This event contained an e-mail address of a user, as well as other unique identifiers named deviceinfo, userinfo, tenantinfo, userobjectid and pipelineacountid.

The event contained the following elements:
Data.AuthorMatch
Data.JobCityMatch
Data.JobStateMatch
Data.JobTitleMatch
Data.JobZipCodeMatch

Microsoft explains that Word scans the contents of documents to detect whether a document is a resume.

> *"How does my resume get detected?*
> *Word scans for patterns in the documents you open, to determine if the document is likely to be a resume--similar to how grammar checking works. If you consent to use Resume assistant, then pattern-matched content from your resume is used to tailor the results in the Resume Assistant pane. For example, a job title and a location name allows for tailored job results. This is used only to enhance the Resume Assistant experience; Microsoft does not collect any personal information."*[42]

Microsoft confirms with this explanation that Office scans the contents of the Word documents to infer whether the document is a resume. The results of such a scan

[41] E-mail Microsoft to SLM Rijk 4 November 2018.
[42] Microsoft, Write your best resume with help from LinkedIn and Resume Assistant, paragraph 'Public profiles and privacy', undated, URL: https://support.office.com/en-us/Article/write-your-best-resume-with-help-from-linkedin-and-resume-assistant-444ff6f0-ef74-4a9c-9091-ffd7a9d1917a?ui=en-US&rs=en-US&ad=US (URL last visited and recorded on 8 July 2019).

were evidently sent to Microsoft via this telemetry message, and possibly other telemetry messages that were not observed.

This behaviour can no longer occur in the new 1905 version of Office 365 ProPlus, if the administrator uses the policy to centrally block the LinkedIn Resume Assistant and other Controller Connected Experiences.

In sum, regardless of the telemetry setting 'Neither' or 'Required, Microsoft collects telemetry events with information that can be considered personal data of a sensitive nature. Even though Microsoft collects the locations and URLs of files in a hashed form, they are personal data of a sensitive nature, as they may contain confidential, restricted or classified information, and/or contain directly identifying personal data. Through the diagnostic data, Microsoft collects detailed statistics about documents and individual user activity. Detailed information about work duration in the four applications can reveal detailed information about employee behaviour. This type of information can be used to provide detailed analytics to employers, as shown in Windows Analytics. Microsoft no longer scans Word documents to detect resumes that can be connected to LinkedIn if the admin has turned off the optional (Controller) Connected Experiences.

2.1.2 Ability to combine events over time

The likelihood of identifiability increases considerably with the ability to link different data events to an individual user. There are three relevant circumstances that allow Microsoft to link different events over time to individual users.

The processing of telemetry processing involves large amounts of data. The telemetry streams are dynamic. Following internal privacy approval, engineers may add new events to the stream. Until 2018 there were no central rules governing the collection of the Office telemetry data.[43]

A second relevant circumstance is the fact all diagnostic data from Office 365 ProPlus and Windows 10 Enterprise are stored long term in the Cosmos database in the USA.[44] Microsoft explains that system-generated event logs are stored in Cosmos as well.[45] More information about Cosmos is provided in paragraph 8 of this report.

In response to the first DPIA report, 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*).

"Accordingly, Microsoft agrees that Cosmos contains personal data within the meaning of Article 4. However, we have access controls in place to ensure that personnel with access only to scrubbed EUII and EUPI in Cosmos are not able to identify natural

[43] See footnote 5, first Office ProPlus DPIA report for SLM Rijk, 7 November 2018, with reference to Meeting report 28 August 2018, answer to Q1. In its response to the initial Office 365 ProPlus DPIA Microsoft has explained that there are rules governing the collection of *new* telemetry events. See paragraph 8 of the initial DPIA report.

[44] "*Cosmos is the central audit record repository for all service teams and audit logs are uploaded to Cosmos from all servers in the Office 365 environment.*" Microsoft Compliance Manager Office 365, tab 'Microsoft Managed', Control ID: 6.9.3. 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 (URL last visited and recorded on 8 July 2019).

[45] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q4f.

persons. The means to re-identify or link a person via look-up tables is handled as Customer Data, subject to rigorous access controls with logged access."[46]

To be clear, Microsoft has emphasized that it does not try to identify or track the behaviour of a single user over time. However, the possibility of establishing such a link is enough for the classification of information as personal data. It is not necessary that this process of combining events leading to identification is actually carried out.

Similarly, Microsoft is technically capable of creating profiles of users and user groups based on the behavioural metadata collected over a period of time. An important result of the negotiations with Microsoft is that the purposes for which Microsoft may process personal data have contractually been limited, regardless whether they belong to the Customer Data or to the diagnostic data. With regard to the services for which Microsoft is a data processor, Microsoft is not allowed to use any of these data for any profiling purpose. This will be described in paragraph 4 of this DPIA.

2.1.3 Ability to use the diagnostic data for analytical services

The ability to combine diagnostic data relating to the behaviour from an individual user over time is not merely theoretical. Microsoft offers three different kinds of analytic services based on the diagnostic data, and Activity Reports in the Microsoft 365 admin center. With MyAnalytics and Delve Microsoft analyses individual work behaviour information and makes the insights accessible for each individual employee, but not for the administrator. Microsoft explains: "*MyAnalytics provides statistics to users to help them understand how they spend their time at work*"[47] and "*Delve uses intelligence to help employees discover relevant content and people across their organization. Users can only see documents they have access to*.[48] SharePoint Online and OneDrive for Business are the primary sources of content in Delve, while MyAnalytics uses email, meetings, calls and chats.

In view of the stated purpose of these two analytic services, the collection of diagnostic data about the use of the Office 365 ProPlus software has as content and as a purpose to identify the individual user. In 2007 the data protection authorities in the EU already explained that for data to relate to an individual, an important threshold for the qualification of personal data, there has to be a "content" element, OR a "purpose" element OR a "result" element.[49] Though the definition of personal data has been expanded in the GDPR to include for example location data and online identifiers, the analysis about the nature of personal data remains valid.

In the case of the different analytic services, the data meet at least the first two element. The DPAs write with regard to content: "*The "content" element is present in those cases where - corresponding to the most obvious and common understanding in a society of the word "relate" - information is given about a particular person, regardless of any purpose on the side of the data controller or of a third party, or the impact of that information on the data subject.*
Information "relates" to a person when it is "about" that person, and this has to be assessed in the light of all circumstances surrounding the case. For example, the

[46] Microsoft confidential response to the initial Office 365 ProPlus DPIA report, 24 September 2018, p. 21.
[47] Microsoft, Office 365 Data Subject Requests for the GDPR.
[48] Microsoft, MyAnalytics privacy guide, paragraph '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 (URL last visited and recorded on 8 July 2019).
[49] Article 29 Working Party, WP 136, On the Concept of Personal Data, p. 10, URL: https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

results of medical analysis clearly relate to the patient, or the information contained in a company's folder under the name of a certain client clearly relates to him."

With regard to purpose, the DPAs write: "*That "purpose" element can be considered to exist when the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual*."[50]

With Workplace Analytics, Microsoft provides organisations with insights about organizational productivity, collaboration patterns, and employee engagement. The processing is based on a user's email and calendar activities, plus additional data that an employer may choose to upload.

According to Microsoft, *Workplace Analytics contains aggregated, de-identified collaboration data of employees*.[51] It follows from a separate explanation about system-generated logs that Microsoft defines de-identified data as pseudonymised 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.*"[52]

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.[53]

Based on the definition in Art. 4(5) of the GDPR, pseudonymised data are personal data.[54] Microsoft also alerts admins that their 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.*"[55]

Employers (and Microsoft) are able through Workplace Analytics to analyse individual work patterns. Thus, the third element of 'result' in the definition of 'relating to' natural persons is met: "*Despite the absence of a "content" or "purpose" element,*

[50] Ibid.
[51] Microsoft writes in its privacy guide voor MyAnalytics: "*Although MyAnalytics is an individual productivity tool, Workplace Analytics enables organizations to view aggregated, **de-identified collaboration data of employees**.*".
[52] Microsoft, Additional steps to export system-generated log data, 6 April 2019, URL: https://docs.microsoft.com/nl-nl/microsoft-365/compliance/gdpr-system-generated-log-data (URL last visited and recorded on 8 July 2019).
[53] 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
[54] Art 4(5) GDPR: " **'pseudonymisation'** ***means the processing of personal data*** *in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;"*
[55] Microsoft DSR, Part 2: Responding to DSRs with Respect to Insights Generated by Office 365, 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).

data can be considered to "relate" to an individual because their use is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case."[56]

2.2 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.

2.2.1 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.[57]

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

If government organisations use SharePoint Online or OneDrive for Business, they have to be aware 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. If the organisation uses an Exchange Online server, Microsoft will log the subject line, as well as all recipients and read the 'open' flag.

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

[56] Article 29 Working Party, WP 136, p. 11.
[57] Amongst others, the categories of classified information are defined in the Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI).

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 continuous 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 and detailed e-mail behaviour. Such monitoring could lead to a negative performance assessment, if not specifically excluded in a workers privacy policy. 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. Though 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 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 the subject lines of e-mails or 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 telemetry data about the location 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. Both servers may collect content data, but the Processor Connected Experiences and the Customer Data (which include subject lines of e-mail) are bound to the new strict purpose limitation agreed by SLM Rijk with Microsoft as a data processor (see paragraph 4.1 of this report).

<u>Special categories of personal data</u>
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.[58]

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.

2.2.2 *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 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.

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

3. Data processing through diagnostic data

As summarised in the introduction and paragraph 1.2 of this DPIA, this DPIA assesses the risks of the processing of diagnostic data *about* the individual use of the Microsoft Office ProPlus software, in combination with Connected Experiences. What are diagnostic data?

In this report, all data *about the individual use of the Office applications and 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 locally installed software that are regularly sent to Microsoft's servers, including the category of data related to the use of Connected Experiences Microsoft calls 'required service data'.

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.*[59]

Contractually Microsoft divides its Office services in two categories: in Core Services and in 'Other' Services. The Office 365 ProPlus software is part of the 'Other' services. Core services are defined in the Online Service Terms.[60] Customer data are all treated as personal data. Microsoft acknowledges that some other types of data may also contain personal data, such as the audit logs or the telemetry data.

Microsoft gives the strongest privacy protections to Customer Data provided in Core Services (such as 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 the EU Standard Contractual Clauses.

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

[60] Microsoft OST May 2019:"*The following services, each as a standalone service or as included in an Office 365-branded plan or suite: Compliance Manager, Customer Lockbox, Exchange Online Archiving, Exchange Online Protection, Exchange Online, Microsoft Bookings, Microsoft MyAnalytics, Microsoft Planner, Microsoft StaffHub, Microsoft Teams, Microsoft To-Do, Office 365 Advanced Threat Protection, Office 365 Video, Office Online, OneDrive for Business, Outlook Customer Manager, Project Online, SharePoint Online, Skype for Business Online, Sway, Yammer Enterprise and Customer's organizational groups managed through the Kaizala Pro admin portal. Office 365 Services* ***do not include Office 365 ProPlus****, any portion of PSTN Services that operate outside of Microsoft's control, any client software, or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or a service branded "for Office 365."* (…)

Customer Data provided through 'Other' services, such as the Office ProPlus 365 software, are audited under ISO 27001. Prior to the negotiations with SLM Rijk the transfer was protected by adherence to the (self-certified) Privacy Shield.

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.[61] As a data controller, Microsoft does not publish audit reports.

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 would like to use the telemetry data to learn that after a user uses backspace, we recommend to use the online dictionary.*"[62]

Since Office 365 ProPlus version 1904, released 29 April 2019, end-users can see the contents of telemetry data collected via the telemetry client in the Office software installed on the end-user device through the Data Viewer Tool. In order to see the contents of other diagnostic data that are collected through system generated server logs, they can also ask their administrator to file a data subject access request through 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 (or hackers). This includes the logs created by the use of the Connected Experiences, Exchange Online, SharePoint Online en OneDrive for Business.[63] The audit logs contain information about for example access to files in SharePoint Online, or the subject line of an e-mail.[64] For an assessment of data subjects rights, see paragraph 15 of this report.

---

[61] Explanation provided by Microsoft in e-mail to SLM Rijk of 1 November 2018.
[62] Meeting report 3 September 2018, new question renumber.
[63] 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.*"
[64] 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-

3.1 Anonymisation and pseudonymisation

Anonymisation is a complex and dynamic form of data processing.[65] 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 365 ProPlus

In the new Office 365 ProPlus versions released since 29 April 2019 (for this DPIA version 1905 was tested) Microsoft provides a number of new choices and settings to government organisations to influence the processing of diagnostic data. The end-users (employees and workers) are also provided with some choices, though many of these choices can be overruled by the administrator.

The four most relevant privacy choices for administrators related to the processing of diagnostic data are:

1. Telemetry level
2. Connected Experiences
3. Integration of LinkedIn accounts with employee work accounts
4. Use of Office 365 Reports in the Admin Center, Workplace Analytics, MyAnalytics and Delve

The processing of diagnostic data is partially influenced by the type of Office deployment: entirely local, hybrid or fully cloud. In line with the government PIA model, these different deployments are discussed in paragraph 8 *Techniques and methods of the data processing*.

---

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.

[65] 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

1. Telemetry setting

Administrators can choose a telemetry setting. If they do not configure this setting, Microsoft by default collects both the highest level of telemetry: Optional, which includes the Required diagnostic data.[66] It is possible to configure the level of client software diagnostic data sent by Office to Microsoft through the Group Policy setting available under User Configuration\Policies\Administrative Templates\Microsoft Office 2016\Privacy\Trust Center.[67]

Microsoft explains: *"As an admin for your organization, you'll be able to use a policy setting to choose which level of diagnostic data is sent to us. Optional diagnostic data will be sent to Microsoft unless you change the setting. Providing optional diagnostic data better enables the Office engineering team at Microsoft to detect, diagnose, and mitigate issues to reduce impacts to your organization.*

Your users won't be able to change the diagnostic data level for their devices if they are signed in to Office with their organizational credentials, which is sometimes referred to as a work or school account."[68]

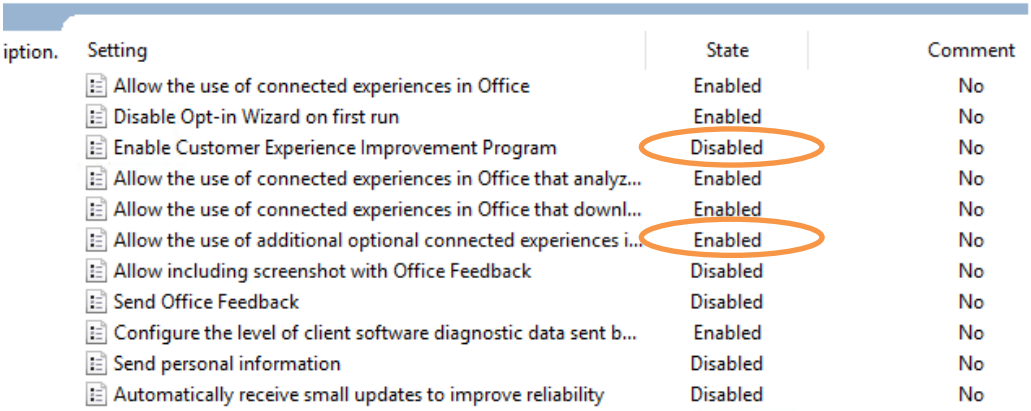
Microsoft also provides a link to the Office cloud policy service, and an overview of the registry settings that admins may enter directly.[69]

2. Prohibit some or all of the Connected Experiences

Administrators also have four options with regard to the diagnostic data collection through the Connected Experiences.

1. Prohibit Connected Experiences that download online content
2. Prohibit Connected Experiences that analyse content
3. Prohibit all Connected Experiences
4. Prohibit the Controller (optional) Connected Experiences

Illustration 3: privacy options for admins



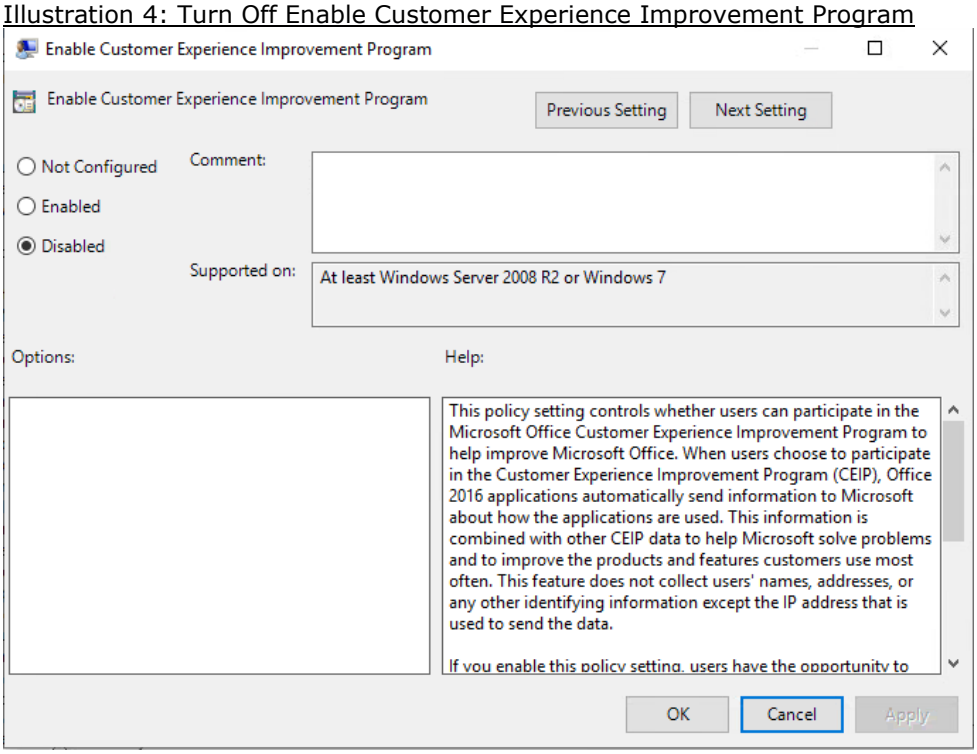
iption.	Setting	State	Comment
	Allow the use of connected experiences in Office	Enabled	No
	Disable Opt-in Wizard on first run	Enabled	No
	Enable Customer Experience Improvement Program	Disabled	No
	Allow the use of connected experiences in Office that analyz...	Enabled	No
	Allow the use of connected experiences in Office that downl...	Enabled	No
	Allow the use of additional optional connected experiences i...	Enabled	No
	Allow including screenshot with Office Feedback	Disabled	No
	Send Office Feedback	Disabled	No
	Configure the level of client software diagnostic data sent b...	Enabled	No
	Send personal information	Disabled	No
	Automatically receive small updates to improve reliability	Disabled	No

[66] Microsoft, Overview of privacy controls for Office 365 ProPlus, 6 May 2019.
[67] Microsoft warns to download and install the Updated Group Policy files from the Microsoft download center. Microsoft Use policy settings to manage privacy controls for Office 365 ProPlus, 6 May 2019.
[68] Microsoft, Overview of privacy controls for Office 365 ProPlus, 6 May 2019.
[69] Microsoft, Use policy settings to manage privacy controls for Office 365 ProPlus, 6 May 2019, Paragraph Privacy related changes to the Office UI, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/manage-privacy-controls#privacy-related-changes-to-the-office-ui (URL last visited and recorded on 8 July 2019).

These policy settings can be implemented by using either Group Policy or the Office cloud policy service.[70]

Government administrators are advised to turn off the setting "Enable Customer Experience Improvement Program". This type of data collection is turned On by default in the new Office 365 version tested in this DPIA. This setting was Off in previous versions, and users were presented with a choice in their privacy options.

Illustration 4: Turn Off Enable Customer Experience Improvement Program



Microsoft has explained that it has removed the option for users om the Trust Center Pane in Office ProPlus to select to send data to Microsoft to help improve customer experience. Microsoft confirms that this default setting for admins has no effect. "*However other software offerings that still offer CEIP will still rely on this policy setting. In the future, if we do work on other software offerings that you use on premises as contemplated in our agreement, we can investigate these case by case together. For now we assume you'll just turn this off since CEIP experiences are optional and have no impact on the core value of any software.*"[71]

The settings for administrators regarding the Connected Experiences, as shown in illustration 3, are highly confusing. The admins must enable the use of all three kinds of Connected Experiences, including the optional Controller Connected Experiences. They must first choose 'enable' before they can actually choose to disable the Controller Connected Experiences.

[70] These policy settings are located under User Configuration\Policies\Administrative Templates\Microsoft Office 2016\Privacy\Trust Center. For the Office cloud policy service see https://docs.microsoft.com/DeployOffice/overview-office-client-policy-service (URL last visited and recorded on 8 July 2019).

[71] E-mail Microsoft to SLM Rijk 19 July 2019.

Illustration 5: To start with, the setting to allow the use of connected experiences must be enabled (top left)

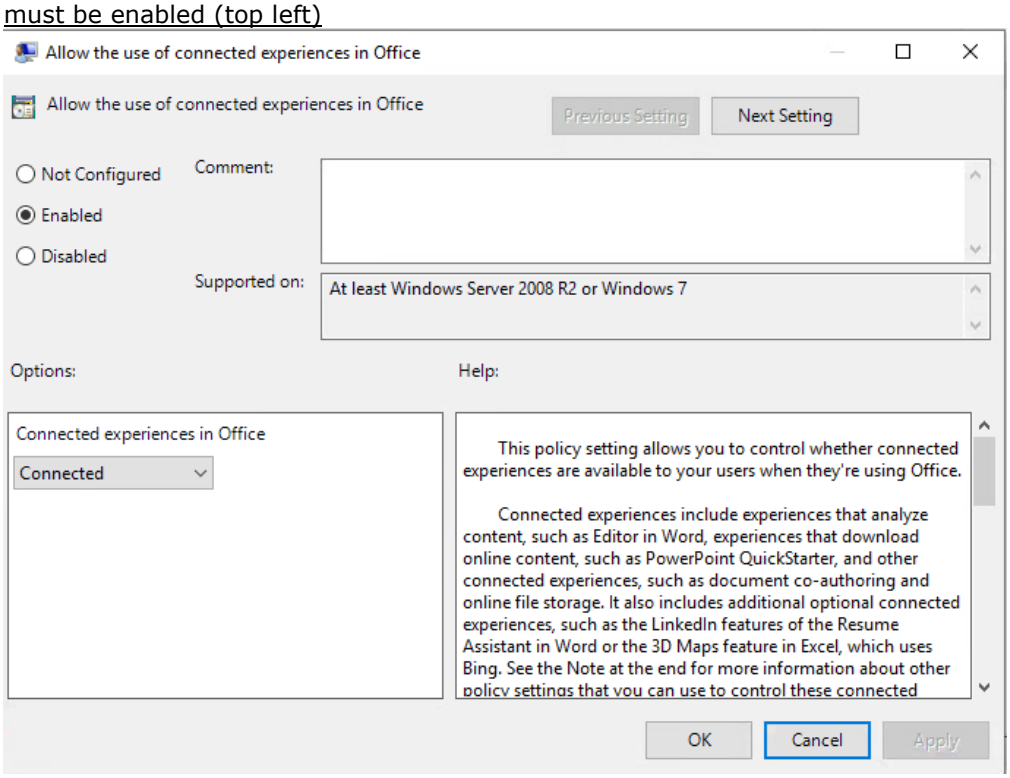
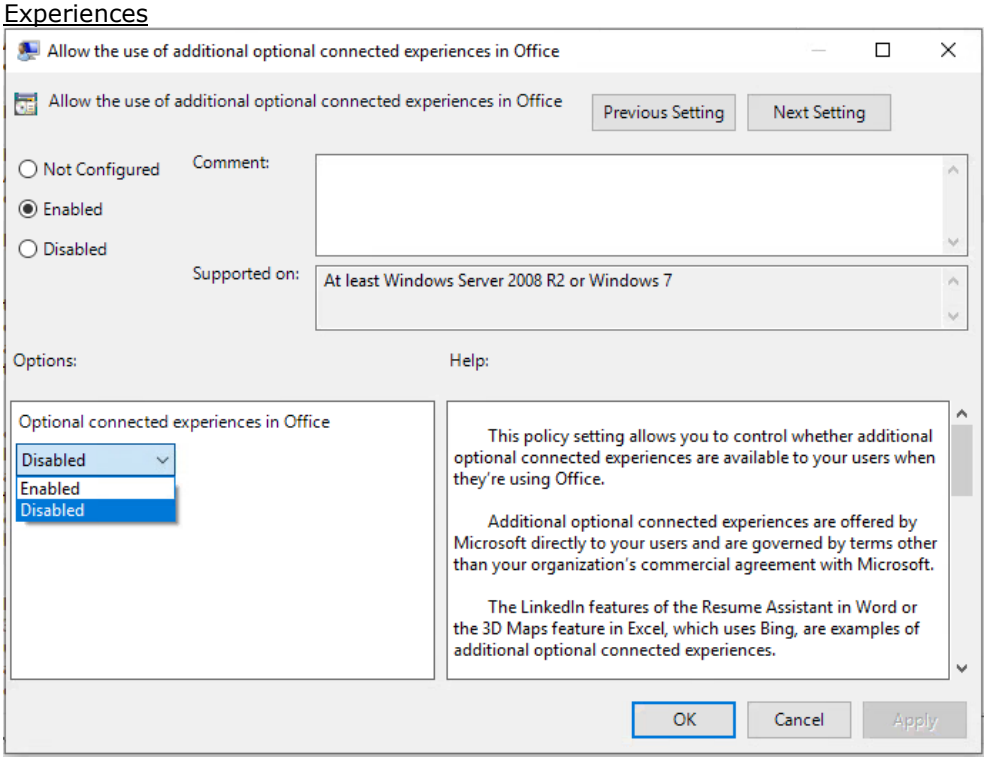


Illustration 6: Select disable in the bottom left square for the Controller Connected Experiences



By default, all Connected Experiences are available. If a user uses a Controller Connected Experience for the first time, in one application, the default setting for all 14 Controller Connected Experiences in all applications in Office is changed. According

to Microsoft this is intentional design (see also paragraph 6.2 of this report, *Interests of Microsoft*. Within Office, the four main applications share tools, and therefore, the consent is configured for Connected Experiences in all Office products.[72]

If the administrator prohibits some or all of the Connected Experiences, either the ribbon or menu command for those connected experiences will be greyed out or the users will get an error message when they try to use those connected experiences.

If the administrator has chosen option 4, to block the Controller Connected Experiences, the user can be shown a warning that the admin has turned off this service:

Illustration 7: Warning (in Dutch) that administrator has turned a specific Connected Experience off[73]

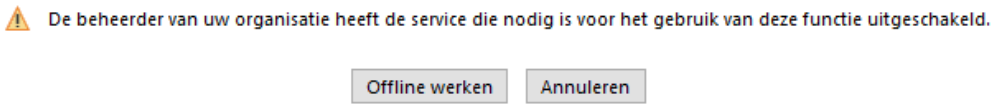


Illustration 8: Warning (in Dutch) that administrator has turned a Connected Experience off[74]

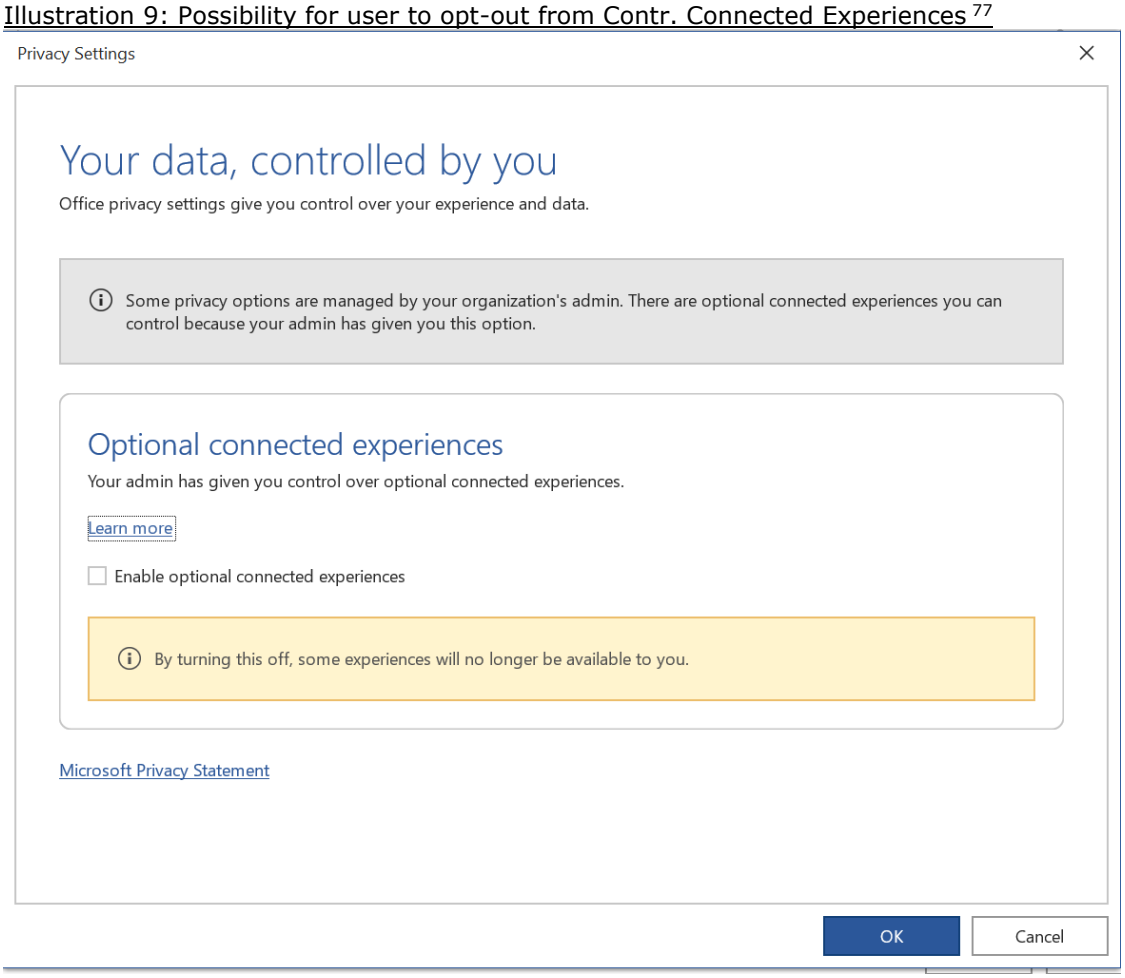
Users of the Office software can access privacy settings through any of the four main applications, through the Options – Privacy Settings, or through the Microsoft Trust Center. Under the tab 'Privacy Options' they see an option to turn on or off the Optional Connected Experiences, if their administrator has not prohibited the use of these services.[75]

Microsoft explains: "*If you have chosen to provide your users with optional connected experiences, the first time your users open an Office app after they've*

[72] Meeting report 3 September 2018, answer to Q4.
[73] For this DPIA the Dutch language version of Office 365 ProPlus was tested. Translated in English, this pop-up says: The admin of your organisation has disabled the service that is necessary for the use of this function.
[74] In English: This experience is not available. The admin of your organisation has disabled the service that is required for the use of this function.
[75] In the previous Office 365 CTR version 1708, Microsoft asked for consent for two types of data processing: send data to Microsoft to improve products and services, and consent to use the Connected Experiences.

been updated to Version 1904, an informational dialog box will appear. This dialog box informs your users that you have given them the choice to use these optional connected experiences and lets them know they can go to File > Account > Account Privacy to change this setting."[76]

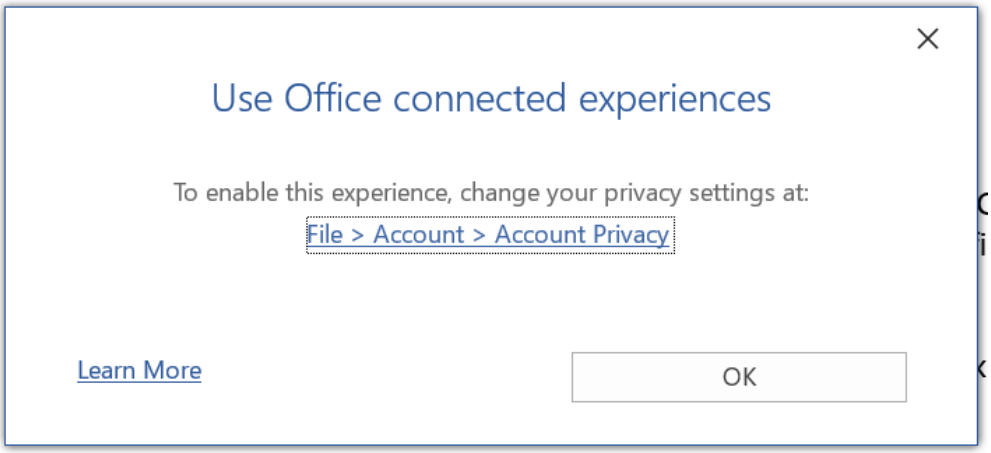
Illustration 9: Possibility for user to opt-out from Contr. Connected Experiences [77]



If the user is not prohibited from using the Controller Connected Experiences, and uses such a service (such as Search) for the first time, the following consent request is shown:[78]

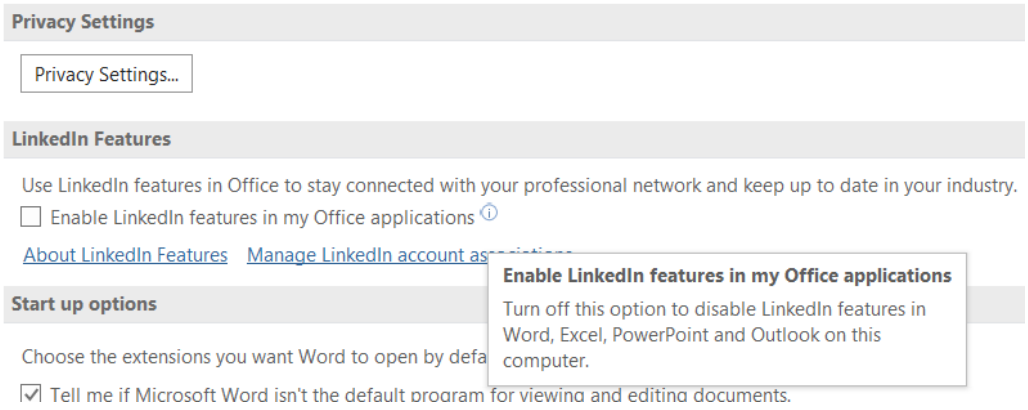
[76] Microsoft, Use policy settings to manage privacy controls for Office 365 ProPlus, 6 May 2019, Paragraph Privacy related changes to the Office UI, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/manage-privacy-controls#privacy-related-changes-to-the-office-ui (URL last visited and recorded on 8 July 2019).
[77] This screen shot was made in Outlook, where the administrator had NOT prohibited the use of the Controller Connected Experiences, and they were thus On by default.
[78] The hyperlinked words 'Meer informatie' point to https://support.office.com/nl-nl/Article/verbonden-ervaringen-in-office-8d2c04f7-6428-4e6e-ac58-5828d4da5b7c?ui=nl-NL&rs=nl-NL&ad=NL (URL last visited and recorded on 8 July 2019).. In English: https://support.office.com/en-gb/Article/connected-experiences-in-office-8d2c04f7-6428-4e6e-ac58-5828d4da5b7c?ui=en-US&rs=en-GB&ad=GB (URL last visited and recorded on 8 July 2019).

Illustration 10: Consent request Connected Experiences



Users also have the option in the privacy settings of Word to use LinkedIn functionality.

Illustration 11: Option for users to switch On LinkedIn functionality



At the page linked via 'About LinkedIn Features' Microsoft explains that turning this setting On enables users to directly see details of their first-degree friends, and work as co-authors in Word and Outlook.[79]

Microsoft explains that administrators may also centrally prohibit integration with the LinkedIn account. In the cloud for the US government, the German cloud and for French tenants, this integration is turned off by default.

Microsoft writes: "*The LinkedIn account connections setting is currently being rolled out to Azure AD organizations. When it is rolled out to your organization, it is enabled by default.*"[80] However, users must first tick the box before their own profile is integrated. "*To see LinkedIn information in Microsoft apps and services, users must consent to connect their own Microsoft and LinkedIn accounts. Users are prompted to connect their accounts the first time they click to see someone's LinkedIn information on a profile card in Outlook, OneDrive or SharePoint Online.*

[79] Microsoft, LinkedIn in Microsoft apps and services, no date provided, URL: https://support.office.com/en-gb/Article/linkedin-in-microsoft-apps-and-services-6d7c5b09-d525-424a-9c18-8081ee7a67e8 (URL last visited and recorded on 8 July 2019).
[80] Microsoft, Integrate LinkedIn account connections in Azure Active Directory, 29 April 2019, URL: https://docs.microsoft.com/en-gb/azure/active-directory/users-groups-roles/linkedin-integration (URL last visited and recorded on 8 July 2019).

LinkedIn account connections are not fully enabled for your users until they consent to the experience and to connect their account."[81]

3. Office 365 Reports, Delve, Workplace Analytics and MyAnalytics

Microsoft provides access for the administrators to the diagnostic data through the Office 365 Reports dashboard and through Workplace Analytics. Microsoft provides access to employees to diagnostic data through MyAnalytics and Delve. Office 365 Reports in the Admin Center, Delve and Workplace Analytics are switched 'On' by default when using Microsoft Office 365.

The analytical services Office 365 Reports, Delve and Workplace Analytics are based on the Office Graph. Administrators cannot turn the Office Graph off. However, they can disable functionality in Office 365 that is powered by the Office Graph, such as Delve, by blocking access to the Office Graph.[82] Access to the Office Graph can be blocked through admin SharePoint settings.[83] Administrators can also prevent viewing reports where user information is identifiable, by changing the privacy settings for all these reports.[84]

Workplace Analytics is turned on by assigning licenses to some or all employees. The default collection settings can be minimised through the admin settings as well.[85]

An important privacy consideration related to Workplace Analytics is that it analyzes email and meeting data from Office 365 and organizational data that the organisation may provide. The standard information includes sender and recipient and date and subject lines for emails; and organizer, attendees, and duration of meetings. Additional data the organisation may provide are HR data such as disciplines, titles, locations, and managers.[86]

Though the data are pseudonymised, reidentification cannot be excluded. Also, Microsoft explains that Workplace Analytics maintains historical organizational data that can include past (previously licensed) employees' de-identified data. New changes (usually monthly) do not affect historical data used by Workplace Analytics.[87]

---

[81] Microsoft, LinkedIn account connections data sharing and consent, 18 March 2019, URL: https://docs.microsoft.com/en-gb/azure/active-directory/users-groups-roles/linkedin-user-consent (URL last visited and recorded on 8 July 2019).

[82] In its privacy guide for MyAnalytics, Microsoft explains that the Microsoft Graph cannot be switched off, but administrators can disable Delve and MyAnalytics separately. "*The Microsoft Graph* ***cannot be turned on or off globally*** *through the Office 365 Admin Center, but administrators can achieve this effect by blocking employees' ability to install third-party apps or by restricting developer access permissions.*" And: "*Administrators and individuals* ***can disable Delve content****-discovery functionality without impacting access to MyAnalytics, and vice-versa.*" And for admins: "*Use PowerShell to* ***opt employees out of MyAnalytics***".

[83] Microsoft, Control access to the Office Graph, 27 June 2019, URL: https://docs.microsoft.com/en-us/sharepoint/delve-for-office-365-admins#control-access-to-the-office-graph (URL last visited and recorded on 8 July 2019).

[84] Microsoft, How do I hide user level details? section in Microsoft, Activity Reports in the Microsoft 365 admin center 7 June 2019, URL: https://docs.microsoft.com/nl-nl/office365/admin/activity-reports/activity-reports?view=o365-worldwide (URL last visited and recorded on 8 July 2019).

[85] Microsoft, Configure Workplace Analytics settings, 24 June 2019, URL: https://docs.microsoft.com/en-us/workplace-analytics/use/settings#admin-settings (URL last visited and recorded on 8 July 2019).

[86] Microsoft, Data-protection considerations when using Workplace Analytics, 21 February 2019, URL: https://docs.microsoft.com/en-us/workplace-analytics/privacy/data-protection-considerations#data-provided-by-your-organization (URL last visited and recorded on 8 July 2019).

[87] Microsoft, Frequently asked questions for Workplace Analytics. 21 February 2019, URL: https://docs.microsoft.com/en-us/workplace-analytics/use/faq (URL last visited and recorded on 8 July 2019).

The service MyAnalytics is based on a combination of Windows 10 Activity History data, mailbox data from Outlook and combined data about the behaviour of other users of Exchange Online (incremental data).
Administrators can prevent users from using MyAnalytics by not assigning licenses to the individual users, but they have to actively change the privacy parameter for the non-licensed users.[88] Microsoft explains: "*Licensed users have MyAnalytics automatically enabled for them after a license is assigned to them. All users in your organization, whether or not they have MyAnalytics licenses issued to them, are opted-in. If you want a licensed user to be opted out by default, which would give them the choice to opt-in, change the value of the PrivacyMode parameter for that user to "Opt-out.*"[89]

An important privacy consideration related to MyAnalytics is to the collection of data about other users of Exchange Online, whether they have 'read' (opened) an e-mail from the sender. Microsoft describes that MyAnalytics, to preserve privacy, does not track read rates for messages sent to fewer than five people and renders the read rate as "Low" or "High.[90] However, this type of data processing still infringes on the privacy of the recipients of the e-mail, as this type of processing can take place without their prior consent and involves observing the reading behaviour of correspondence. The right to privacy of correspondence is a separate fundamental right in the EU, protected by Article 7 of the Charter of Fundamental Rights, the ePrivacy Directive, and in the Netherlands, by the Constitution, Article 13, as well.

4. Purposes of the processing

Prior to the negotiations between SLM Rijk and Microsoft, Microsofts contractual framework did not define diagnostic data, or provide separate data protection guarantees. The same set of eight purposes applied to the processing of the Customer Data and 'other' personal data.

These eight purposes were:
1. Security (identifying and mitigating security threats and risks as quickly as possible through updates to Office ProPlus Applications and remediation of connected services)
2. Up to Date (delivering and installing the latest updates to the Office ProPlus Applications without disruption to the experience)
3. Performing Properly (identifying and mitigating anomalies, "bugs," and other product issues as quickly as possible through updates to the Office ProPlus Applications and remediation of connected services) [91]
4. Product development (learning to add new features)
5. Product innovation (business intelligence, develop new services)
6. General inferences based on long-term analysis (to support machine learning)
7. Showing targeted recommendations on screen to the user
8. Purposes Microsoft deems compatible with any these seven purposes.[92]

[88] Microsoft, MyAnalytics setup for Office 365 Administrators, 11 April 2019, URL: https://docs.microsoft.com/en-us/workplace-analytics/myanalytics/setup/mya-setup-checklist (URL last visited and recorded on 8 July 2019).
[89] Ibid.
[90] Microsoft, MyAnalytics privacy guide, 9 May 2019, Paragraph 'Incremental Data', URL: https://docs.microsoft.com/en-us/workplace-analytics/myanalytics/overview/privacy-guide#windows-10-activity-history-data (URL last visited and recorded on 8 July 2019).
[91] These three purposes were explained in Microsoft's confidential response to the first Office DPIA report for SLM Rijk, 24 September 2018, p. 5.
[92] Microsoft has confirmed on 1 October 2018 that the company may use diagnostic data for the secondary purposes to improve existing Office ProPlus Application functionality. Therefore, the

In its response of 1 October 2018 to the initial Office 365 ProPlus DPIA report, Microsoft explained that the company processed the personal data contained in the system-generated event logs for the same purposes as the Customer data, and this included all compatible purposes.[93] Microsoft only denied that it would do any further processing of content data collected through the Processor Connected Experiences.[94]

These eight purposes only applied (prior to the negotiations with SLM Rijk) to the diagnostic data from services for which Microsoft considers itself to be a data processor.
With regard to the diagnostic data about the use of the (optional) Controller Connected Experiences, Microsoft considers itself to be a data controller, and processes diagnostic data about the use of the services for all of the purposes mentioned in its general Privacy Statement.[95]

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.[96] 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*."[97] As a hyperscale tech provider Microsoft does not conclude individual data processing agreements with its Enterprise customers. Instead, the standard terms and conditions of Microsoft apply. When a customer wishes to change the instructions, the changes to these instructions are applied in the same way as changes to the licensing agreement.[98]

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.

In the specific contract with the Dutch government, Microsoft repeated that the contract and use of features provide a complete list of instructions:

---

initial DPIA report assumed that Microsoft processed the diagnostic data for the 8 purposes mentioned above.

[93] Microsoft claims that the purposes would be clarified in its OST, the section entitled "Processing of Customer Data; Ownership" and the section entitled "Processing Details" in Data Protection Terms, 3rd bullet. The first section states: *Customer Data will be used or otherwise processed only to provide Customer the Online Services* ***including purposes compatible with providing those services****. Microsoft will not use or otherwise process Customer Data or derive information from it for any advertising or similar commercial purposes*. The second section states: *The nature and purpose of the processing shall be* ***to provide the Online Service*** *pursuant to Customer's volume licensing agreement*.

[94] Ibid, p.

[95] 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.

[96] Microsoft European Union model clauses backgrounder, January 2017, URL: https://aka.ms/eu-model-backgrounder (URL last visited and recorded on 8 July 2019).

[97] 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'.

[98] OST May 2019, p. 8.

"*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."*[99]

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.[100]

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

1. Limitation to three purposes

As a data processor for Office 365 ProPlus, 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.

The OST generally describe Microsoft's activities as a data processor. However, with regard to some additional, discretionary Connected Experiences, Microsoft considers itself to be a data controller.

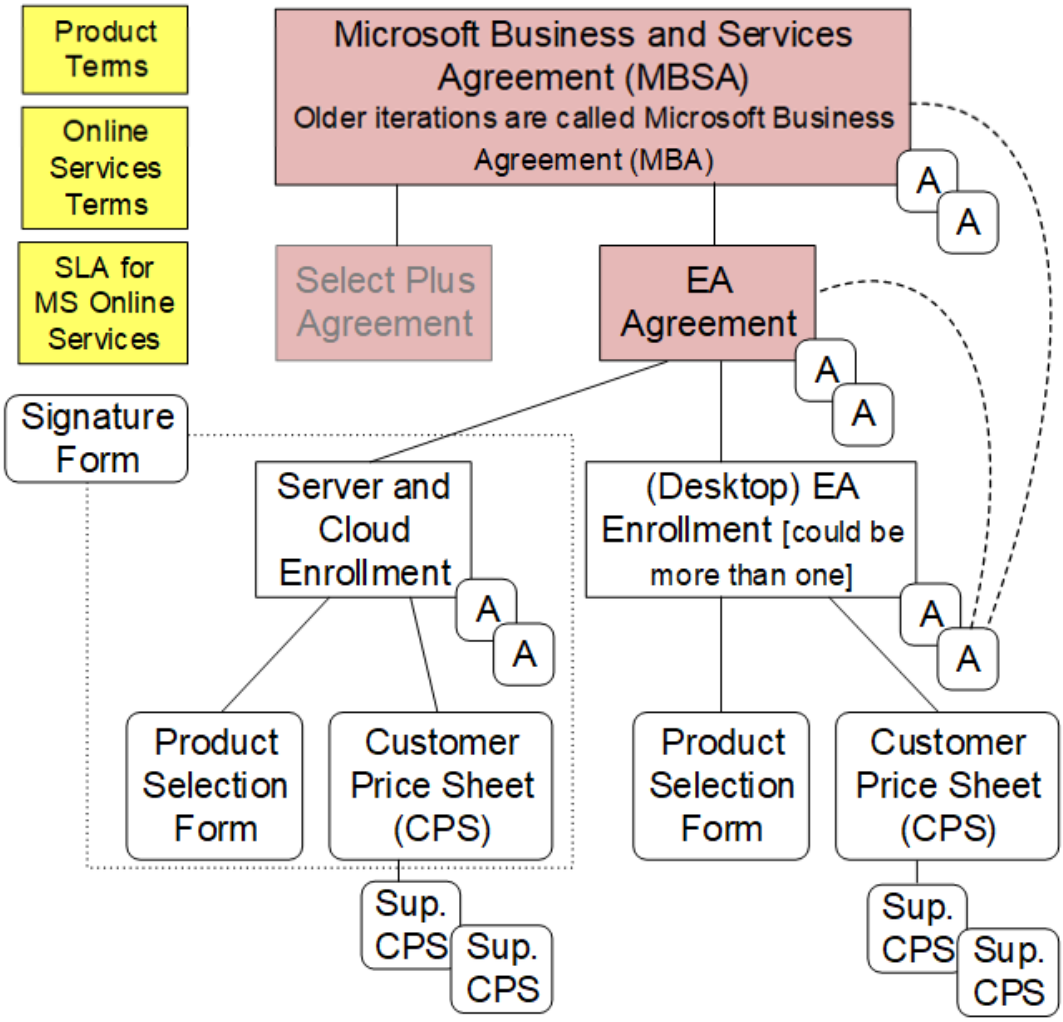
Normally, when a customer wishes to change the instructions for the processing, the changes to these instructions are applied in the same way as changes to the licensing agreement.[101]

As a hyperscale tech provider Microsoft does not conclude individual data processing agreements with individual Enterprise customers. Instead, the standard terms and

[99] Additional GDPR Terms included in Annex 1 to the GDPR Terms, Amendment ID M434, April 2017.
[100] 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.
[101] OST May 2019, p. 8.

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.[102] 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*."[103]

Illustration 12 Contents of enrolment framework Office 365[104]



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,

[102] Microsoft European Union model clauses backgrounder, January 2017, URL: https://aka.ms/eu-model-backgrounder (URL last visited and recorded on 8 July 2019).
[103] 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'.
[104] Graphic made by Directions on Microsoft, URL: https://www.directionsonmicrosoft.com/

including the differences between Microsoft Ireland as the office signing the contract, and Microsoft Corporation as a data controller in the general 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 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.

As a data controller, Microsoft may be obliged to hand over personal data to law enforcement and security agencies / secret services, for example under the CLOUD Act and under FISA orders. Through the amendment negotiated with SLM Rijk, it is clarified that Microsoft does not act as a data processor when ordered to hand over personal data (be it content, or diagnostic data) to a law enforcement authority or security 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 Controller Connected Experiences

Microsoft considers itself to be a data controller when processing diagnostic data from the 14 Controller Connected Experiences. In that case all the purposes mentioned in Microsoft's general Privacy Statement apply.[105]

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.[106]

4.2.1 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."*[107]

4.2.2 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 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.*

[105] Microsoft explains in the OST: *Additionally, if permitted by Customer, users may elect to use connected services subject to terms of use other than this OST and with respect to which Microsoft is a data controller, as identified in product documentation*.
[106] These are the following purposes: Customer support, Promotional communications, Transacting commerce.
[107] Microsoft Privacy Statement, Product-specific details: Enterprise and developer products.

We also communicate with you to secure our products, for example by letting you know when product updates are available."[108]

4.2.3 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.*"[109]

4.2.4 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.*"[110]

4.2.5 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.*"[111]

4.2.6 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.*"[112]

4.2.7 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.*"[113]

4.2.8 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,*

[108] Microsoft Privacy Statement, How We Use Personal Data.
[109] Ibid.
[110] Ibid.
[111] Ibid.
[112] Ibid.
[113] Ibid.

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."[114]

4.2.9 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."*[115]

4.2.10 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."*[116]

4.2.11 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."*[117]

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 diagnostic data from 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."*[118]

4.2.12 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."*[119]

[114] Ibid.
[115] Ibid.
[116] Ibid.
[117] Ibid.
[118] Ibid.
[119] Ibid.

4.2.13 *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.*"[120]

4.2.14 *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.*"[121]

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.

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

1. Microsoft as a data processor, the individual government tenant as a data controller
2. Microsoft as a data controller, the individual government tenant 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

The conclusion of the first Office 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

[120] Ibid.
[121] Ibid.

clarified in two recent rulings[122] and an advice from the Advocate General[123] 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.

Even though the first scenario was the most desirable with regard to all Office diagnostic data, based on a factual and formal analysis, at the time Microsoft did not behave like a data processor with regard to any of the diagnostic data.

Prior to May 2019 there was no comprehensive documentation what kind of personal data Microsoft processed about the individual usage of the Office software, or data viewer tool to decode the diagnostic data, and no clearly defined purposes. Therefore, in practice the government organisations could not fulfil their role as data controllers for the diagnostic data. The alleged 'data controllers' had no clue what personal data the alleged 'data processor' processed on their behalf. Microsoft itself had determined eight purposes of the processing, including the right to decide what other purposes would be compatible for the processing of diagnostic data.

Only data controllers can determine what personal data may be processed for what purposes. A data controller may hire a technology company and outsource certain complicated data processing tasks, such as ensuring the security of the processing, or providing a well-functioning, bug free service. In order to achieve such clear objectives, the data processor has a certain liberty to decide how the personal data are processed, in what systems (with what *means*). However, Microsoft had contractually maximised this liberty, and provided no well-defined, clearly delineated purposes that would allow the government organisations to be in control.

The third scenario (Microsoft as a unique data controller) only theoretically applied to the collection of diagnostic data about the use of some Connected Experiences. Given the (then) lack of transparency, the lack of central policies to turn off the Controller Connected Experiences and the undesirability of turning off indispensable services such as the spelling checker, the government organisations were also joint controllers for the processing of diagnostic data about the use of (all) Connected Experiences.

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.[124] Additionally, all Office telemetry data are sent to a single

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

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

[124] 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

end-point in the USA, where engineers from Microsoft Corporation may use the diagnostic data for analysis purposes.

5.1 Results of negotiations Microsoft as data processor

As a result of the contractual purpose limitation agreed with Microsoft, Microsoft no longer itself determines purposes for the processing of the diagnostic data. Microsoft has committed to only process personal data for purposes that are determined by the data controllers, the Dutch government organisations that use Office 365 ProPlus.

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, 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'.

Effective audit right

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.[125] 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. Though 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.

Contracts with 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.[126] Microsoft is now

---

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.

[125] 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.

[126] Meeting report 30 August 2018, answer to Q41.

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.[127] 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.*"[128]

Determining the 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.*"[129]

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 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 comply with an order from 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.[130]

Microsoft publishes a bi-annual transparency report. In the Netherlands, in the period July-December 2018, Microsoft received 176 law enforcement requests, relating to

[127] Microsoft overview OST sub-processors, 5 March 2019, URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2ouXb
[128] Meeting report 30 August 2018, answer to Q40.
[129] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q8 (preamble).
[130] Meeting report 30 August 2018, answer to Q40 and Q41.

222 accounts/users.[131] Microsoft explains that very few law enforcement requests relate to Enterprise cloud customers.[132] 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.

Though 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).[133]

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.*"[134]

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.[135]

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.*"[136]

This promise does not apply to the diagnostic data from the Controller Connected Experiences, because the OST do not apply. In its 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.*"[137]

When Microsoft is obliged itself to hand over personal data to law enforcement and security agencies / secret services, for example under the CLOUD Act and under FISA orders, Microsoft acts as a data controller, not 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. Microsoft can be ordered to provide access to the data to US authorities, regardless

[131] 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).
[132] 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*.
[133] 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.
[134] OST May 2019, p. 7.
[135] Ibid.
[136] Ibid.
[137] Microsoft general privacy statement, last updated June 2019.

whether they are still stored in data centres in the EU, or already transferred to the USA for commercial purposes.

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 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).*"[138]

The Dutch government organisations clearly cannot instruct Microsoft to process data in violation of the GDPR, when complying 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

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. If the administrator has not prohibited the use of these services, Microsoft processes the diagnostic data based on the consent of the end-user, the government employee.

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. To mitigate the confusion, Microsoft has publicly explained the differences between the different Connected Experiences. Microsoft has also provided different options for administrators to centrally prohibit all or some of the Connected Experiences.

If government organisations would allow their employees to consent to data processing for the Controller Connected Experiences, they would become joint controllers with Microsoft for the processing of personal data about the use of these services. The only way the government organisations can prevent this joint controllership, is by switching off the Controller Connected Experiences completely.

The different legal grounds in relation to the roles of Microsoft as data processor and (sole) data controller will be analysed in paragraph 11 of this report.

[138] 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

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 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 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.[139] 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 (…).*"[140]

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.*"[141]

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 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."*[142]

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

[139] 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/.
[140] Idem.
[141] Meeting report 30 August 2018, answer to Q46.
[142] Meeting report 29 August 2018, answer to Q16.

Experiences was default switched to "off".[143] 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.[144] Microsoft writes in its 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***."[145]

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.[146] 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.[147]

6.3 Joint interests

The interests of Microsoft and the Dutch government align when it comes to the use of diagnostic data to protect the integrity, availability, and reliability of personal data in its services. As part of the shared security interest, the provision of technical updates by Microsoft also concurs with the interests of the Dutch government organisations, provided that the updates do not disrupt the service and that the technical administrators are able to disable or adjust the updates.[148] 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. Through the Privacy Shield (previously Safe Harbour) US American undertakings may 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

[143] Meeting report 29 August 2018, answer to. Q30.
[144] 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.
[145] Idem, p. 10.
[146] Meeting report 29 August 2018, answer to Q21.
[147] Meeting report 29 August 2018, answer to Q21.
[148] 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.

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.[149] Though 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.[150]

In its OST[151], 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.*"[152]

Microsoft details the different data centres it uses for the different Office 365 services. The actual storage in different data centres 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.[153]

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.

[149] Microsoft is an active participant in the Privacy Shield Framework https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK&status=Active
[150] 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 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.
[151] Microsoft Online Service Terms Microsoft, May 2019.
[152] Idem, p. 10.
[153] Microsoft, Where is your data located, URL: https://products.office.com/nl-NL/where-is-your-data-located?ms.officeurl=datamaps&geo=Europe#Europe

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).*"[154]

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.*[155] Additionally, the data protection authorities refer to the ongoing negotiations about an international agreement between the EU and the US on cross-border access to electronic evidence for judicial cooperation in criminal matters and negotiating directives.[156]

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 of this report (*Retention Periods*). Access to the Customer Data that Microsoft defines as Core Online Services is audited following the strict controls of SOC-2.

The actual storage in the different data centres varies per service. This is for example different for Outlook and for SharePoint Customer Data. The diagnostic data from the different Office 365 products and services are sent to, or collected directly on, Microsofts servers in the USA. Technically, the diagnostic data from the Office software are sent through one unified telemetry API, and sent to several endpoints in the USA.

Microsoft does not publish public documentation about the Office network endpoints for the diagnostic data. Microsoft only publishes two lists of network endpoints for Windows, for the Windows consumer and professional versions, and for the Windows Enterprise versions.[157] Both lists contain different network endpoints for Office

[154] 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
[155] Idem, cover letter.
[156] 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
[157] 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

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, because 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

Microsoft collects diagnostic data about the use of its Office software in multiple ways, for example through the separate telemetry client built in its operating system Windows. This type of data processing was addressed in an earlier DPIA commissioned by SLM Rijk. Separate from the telemetry data from Windows 10, Microsoft also collects diagnostic data through a separate telemetry client in the locally installed Office software and through system-generated event logs.

As explained in the introduction, Privacy Company has analysed the telemetry events captured with the Data Viewer Tool by the test lab created by SSC-I for the Ministry of Justice and Security.

The telemetry client inside the Office software collects events about the usage of the software and stores these snapshots on the device. Similar to the way in which Microsoft collects telemetry data about the use of Windows 10, 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 Office to Microsoft, to limit the use of the end-user's device resources.[158]

It is not known how frequently the software captures data, or how frequently the client transmits the collected data to the Microsoft servers. Technically, the diagnostic data from the Office software are sent through one unified telemetry API, and sent to one endpoint in the USA.[159] Through this telemetry client, Microsoft also collects diagnostic data about the use of both kinds of Connected Experiences.

Besides the processing via the telemetry client, Microsoft collects diagnostic data via system-generated event logs on its cloud storage and email servers (SharePoint Online, OneDrive for Business and Exchange Online). Part of these event logs are reflected in the security audit logs.

Additionally, Microsoft collects diagnostic data from system generated logs about the use of the processor Connected Experiences.

8.1 Local versus hybrid cloud use of Office software

Government organisations can use the Office 365 ProPlus software 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.

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

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

In the first case, Microsoft collects telemetry data from the in-built telemetry client about the use of the Office software and diagnostic data from its cloud servers relating to the use of the Connected Experiences. Since May 2019, Microsoft provides administrators with a choice regarding the level of telemetry. Microsoft also publishes extensive documentation about the contents of the telemetry data.

In the second scenario, Microsoft collects additional personal data through system-generated server logs related to its cloud storage and mail services. Customers can gain some understanding of the contents of these data by filing a Data Subject Request, and by examining the audit log files. 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 365 ProPlus, 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.*"[160]

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*

[160] 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

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."[161]

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

Until May of 2019, Microsoft did not provide comprehensive documentation about the content of the diagnostic events collected by the use of the Office software and Connected Experiences.
Microsoft has also explained that until recently, there were no central rules governing the collection of telemetry data.[162] 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."* [163]

With Office telemetry Microsoft estimated it collected data on a much larger scale than in Windows 10 telemetry. "*Office telemetry contains between 23 and 25 thousand events, as opposed to 1.000-1.200 events for Windows 10. While Windows 10 telemetry is controlled by maybe 8 to 10 engineers, Office telemetry is in the hands of 20-30 engineering teams.*[164]

Microsoft has not provided information about rules governing the collection of information through the Controller Connected Experiences.

Microsoft stores the telemetry data from both Office and Windows together with diagnostic data from its cloud services in the central long-term database Cosmos. A former Microsoft engineer explains the architecture of Cosmos in a slideshow, and explains that Cosmos not only contains these data, but also data from Skype, Xbox, Bing Ads and more.[165] 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.*"[166]

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*

[161] Ibid.
[162] Meeting report 28 August 2018, answer to Q1.
[163] Microsoft confidential response to first Office 365 ProPlus DPIA report, 24 September 2018, p. 10.
[164] Meeting report 28 August 2018, answer to Q1.
[165] 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)
[166] Ibid, slides 8 and 13.

– *Long tail of other data sets of interest*"[167]

As quoted in paragraphs 4.2.10 and 4.2.11 of this report, Microsoft contractually permits itself as a data controller for the Controller Connected Experiences to analyse data from different sources to predict interests and to send users 'relevant offers' and show targeted advertisements in Microsoft products and services, and on third party websites.

Though the data processing remains dynamic, Microsoft has published extensive documentation in the new versions of Office 365 ProPlus released since 29 April 2019, and more importantly, made the Data Viewer Tool available for admins to inspect the Office ProPlus telemetry data.

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.[168]

[167] 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).

[168] 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*."

On 10 January 2017, the European Commission published a proposal for a new ePrivacy Regulation.[169] 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.[170] It added a specific exception on the consent requirement to provide updates as well as an 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.[171] 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.[172] 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

[169] 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.
[170] 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.
[171] 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.
[172]. 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.

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;[173]

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: [174]

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.
(…)

[173]. 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.
[174] Ibid.

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 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.[175]

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.[176]

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.

[175] 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.

[176] Microsoft, Data Retention, Deletion, and Destruction in Office 365, 6 May 2019, URL: https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-data-retention-deletion-and-destruction-overview.

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. 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.[177]

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

"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 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 from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.*"[178]

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*

[177] Microsoft confidential answer 1 October to the 10 follow-up questions, answer to Q4b.
[178] 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).

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."[179]

Microsoft does not offer a possibility to delete outdated Office telemetry data 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.[180]

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.[181] 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.*"[182] 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."[183]

[179] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q8 (preamble).
[180] Ibid, answer Q8b.
[181] Meeting report 30 August 2018, answer to Q33.
[182] Microsoft, Data Retention, Deletion, and Destruction in Office 365, 6 May 2019.
[183] 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 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. In its role as data processor, Microsoft can rely on the relevant legal grounds of the Dutch government organisations for the data.

The only exception, where Microsoft does not behave as a data processor, is the data processing relating to the optional Controller Connected Experiences. As described in paragraph 4.2 of this DPIA report, Microsoft acts as a data controller for these services, and contractually permits itself to process the diagnostic data for 14 purposes from its Privacy Statement. If the government organisations do not centrally block access to these services, they are joint controllers with Microsoft for the processing of the diagnostic data about the use of these services, and the government organisations must have a legal ground for the data processing.

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 along with 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*".[184] Therefore, with regard to the Controller Connected Experiences, five of the six legal grounds can theoretically apply to the processing of diagnostic data. Only the ground of vital interest is not discussed, since nor Microsoft nor the government have a vital (lifesaving) interest in the processing of the diagnostic data.[185]

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

This legal ground is not applicable, 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

[184] Microsoft Privacy Statement, Personal Data We Collect, June 2019.
[185] 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.

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 optional (Controller) Connected Experiences.

If the administrators of the government organisations do not centrally prohibit the use of these optional Controller Connected Experiences, employees are asked for consent by Microsoft the first time they access such as service. See illustrations 9 and 10 in this report, with the different privacy options for end-users.

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. An option to switch off certain data processing can never meet the requirements from the definition of consent that it must be a *clear affirmative action*, and an *unambiguous indication of the data subject's wishes*. A failure to exercise an opt-out option can only be interpreted as inactivity and recital 32 of the GDPR specifies: *"Silence, pre-ticked boxes or inactivity should not therefore constitute consent*."

Additionally, 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

Employees must use the Office products to be able to carry out the tasks included in their job description. Hence, to the extent that the processing is strictly necessary for the performance of the contract which the data subject has with the governmental organisation, the organisation may successfully appeal to this legal ground. As a result of the negotiations, Microsoft has agreed to only process the personal data in and about Office 365 ProPlus for three purposes, and has limited the amount of personal data it collects.

It is not evident that all diagnostic data at the Required level of telemetry are strictly necessary for the performance of the contract (from government) with the user. Simply put: if there is an opt-out for some of the data, the processing of these is not strictly necessary. Since Microsoft also offers a setting to not collect diagnostic data from the applications running on the device (telemetry set at 'Neither'), it is obviously possible to meet the three purposes without all of the data at the Required level. Therefore all data that are collected on top of the minimum standard 'Neither', do not comply with the requirement of strict necessity.
The requirement of strict necessity for all data and for all purposes is addressed in the next paragraphs 13 and 14 of this report (purpose limitation and necessity).

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

In its response to the first DPIA Microsoft claimed it could rely, as a joint controller, on the legal ground of contract, since employees would freely sign a separate contract with Microsoft by ticking the box to use the optional (Controller) Connected Experiences.[186] This argument is 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 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 in the GDPR of necessity to process specific personal data to perform a contract. As outlined above, without comprehensive documentation, Microsoft is unable to demonstrate the necessity of the processing of the diagnostic data currently stored and collected on an ongoing basis.

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].[187]

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."[188]

[186] Microsoft confidential response to the initial Office 365 ProPlus DPIA report, 24 September 2018, p. 16 and 17.

[187] 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].

[188] Idem, paragraphs 49 and 50, page 13.

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.[189] 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

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, 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 optional (Controller) Connected Experiences.

Nor Microsoft nor the government organisations are subjected to any specific legal obligation to process diagnostic data about 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

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 optional (Controller) Connected Experiences.

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.

[189] 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.

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

Article 6(1) f reads as follows: "*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

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 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 optional (Controller) Connected Experiences.

It follows from Microsofts 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). 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.

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 party makes a device give access via the internet to stored data on the device. Preceding the analysis of necessity, the special character of the diagnostic data 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.

However, these legal grounds are not available for the processing of sensitive data through the (optional) 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. Therefore, the government organisations must prohibit employees from using the optional Controller Connected Experiences.

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, incl. 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	√	√
Other purposes in Privacy Statement (only for the optional Controller Connected Experiences)	Consent	X	X
	Contract	X	X
	Legal obligation	X	X
	Legitimate interest	X	X

12. Special categories of personal data

As explained in paragraph 2 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.*"[190]

The EDPS refers to the criteria provided by the Article 29 Working Party when a Data Protection Impact Assessment (DPIA) is required.[191] 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 certainly 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.

[190] 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

[191] 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 .

As described in paragraph 5.2, Microsoft and the government organisations that allow the use of the optional (Controller) Connected Experiences 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.

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. Since, Microsoft has created policy rules, has performed a major overhaul of the inventory of telemetry events and has made a major effort to inform users about the categories of personal data and specific purposes for which Microsoft uses these data.

Most importantly, Microsoft has agreed in May 2019 as a data processor to limit the data processing to three authorised purposes, and only where proportional. As described in paragraph 4.1 of this DPIA, Microsoft will only process the diagnostic data from Office 365 ProPlus to provide and improve the service, to keep the service up-to-date and secure.

Microsoft wanted to keep the current broad purpose 'providing the service'. In the past, this purpose was given a very broad interpretation by Microsoft engineers, to include at least 6 other purposes. To prevent such purpose creep, Microsoft has provided additional contractual guarantees and limitations.

Microsoft has guaranteed that it won't use the content data or the diagnostic data for the purposes of profiling, data analytics, market research or advertising, unless the customer explicitly requests Microsoft to do so. This could be the case if a government organisation would choose to use Workplace Analytics.

Microsoft has also defined the specific purposes of data processing that are necessary for legitimate business operations, for which Microsoft is a data controller. These purposes range from the obvious (sending invoices, creating statistics for the annual financial reports) to the often forgotten, such as complying with orders from law enforcement. Microsoft has agreed to anonymise data following the guidelines of the European Data Protection Authorities, as described in Opinion WP216, and not re identify any anonymised data. Microsoft has also agreed not to use any data that it

processes as part of Microsofts legitimate business operations or personal data that are derived from such data, for any other purpose.

The importance of this contractual purpose limitation to lower data protection risks for data subjects, in combination with an effective right to verify compliance, cannot be overestimated.

In the previously examined version 1807 of Office 365 ProPlus, as decoded by Privacy Company, Microsoft apparently routinely matched contents of Word documents to infer if the document was a resume, to prepare for the use of the LinkedIn Resume Assistant. During the execution of the tested scenarios, the tester did not have a LinkedIn account, and Microsoft did not ask for consent to scan the document for this specific purpose. The scanning happened without any question for consent to use the Controller Connected Experience Resume Assistant.

There was no obvious necessity for Microsoft to collect this type of information via a telemetry event. This event thus provides a clear and factual example of the problems and risks that have been described in the initial Office ProPlus DPIA regarding the lack of purpose limitation, as well as the (dis)proportionality of the data processing.

Another clear benefit of the negotiations is that Microsoft can no longer itself determine what purposes would be *compatible* with the three newly agreed purposes. As quoted in paragraph 6 of this report, about the different 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 wanted to present targeted recommendations on screen in Office. As explained in the first Office 365 ProPlus DPIA report, this was one of the purposes which Microsoft deemed compatible with the overall purpose of 'providing the service'. This specific form of advertising has been explicitly prohibited in the amended contract with SLM Rijk.

The example shows that the previous purposes were 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.[192]

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.

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 on the audit logs, 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, OneDrive for Business and Exchange Online). As highlighted in paragraph 2.1.1 of this report, 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,[193] but seems to work with a very broad definition of Connected Experiences, to include the use of Teams and all cloud services. Microsoft does not provide an overview either of the diagnostic data that are generated in system logs on Microsoft's servers that provide the Connected Experiences.

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 365 ProPlus diagnostic data.

[192] 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).*

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

Since version 1904 of Office 365 ProPlus, released 29 April 2019, Microsoft provides administrators with two choices with regard to the content and volume of diagnostic data.

Administrators can opt-out from the default telemetry level of 'Optional' and choose to set the diagnostic data collection to 'Required' or 'Neither'. As described in paragraph 2.1.1, there are not many differences between the two levels. The observed telemetry data do not contain any content from documents, emails or conversations, and no directly identifying data such as user names or e-mail addresses. The events related to the use of the processor Connected Experiences such as the spelling checker and Translator also do not contain snippets of content.
However, at the Required level some information is collected of a more sensitive nature, while the collection of these data is not necessary (because these data are not collected at the level 'Neither').

Government administrators may also choose to turn off some or all of the Connected Experiences. This is mandatory with regard to the Controller Connected Experiences, if the organisations do not want to risk processing personal data for unlawful purposes. As assessed in paragraph 12 of this report, there is no legal exception for Microsoft as joint controller with the government organisations to lift the legal prohibition on the processing of these data for all 14 purposes of the Privacy Statement. However, following the analysis in paragraph 11, there is no legal ground either for the processing of 'regular' personal data in the Controller Connected Experiences.

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. They 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 defined in its Privacy Statement.

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 Windows and Office are stored 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.

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 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, this freedom was limited or non-existent. In practice, government organisations have been working for a very long time with Microsoft Office products. 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.

In sum, there are no directly equivalent alternatives that can be deployed by government organisations that present less data protection risks.

With regard to secret data, special categories of data or otherwise very sensitive data, government organisations should consider using purely local, on-premise Office software without a Microsoft account. However, this is not a long term alternative, since many government organisations have already bought Office 365 functionality, because they want to use relevant new functionality. In the end all organisations are forced to update to Office 365 (in October 2020 at the very latest), as the support lifetime of older Office versions expires.

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. In the second DPIA about these mobile and online versions of Office 365, published simultaneously by SLM Rijk, it is concluded there are five high data protection risks. First of all, it is impossible to centrally prohibit the use of the Controller Connected Experiences in Office Online and the mobile Office apps, and second, Microsoft qualifies itself as data controller for the diagnostic data processing from the mobile Office apps, and thus contractually permits itself to process these data for all 14 purposes from its Privacy Statement.

15. Data Subject Rights

The GDPR grants data subjects a number of rights.

Right to information
First of all, data subjects have a right to information. This means that controllers must provide the data subject with easily accessible, intelligible, concise information in clear and plain language about, among other things, the identity of the controller, the data processing activity, the intended duration of storage, and the rights of the data subject.

As has been highlighted in previous paragraphs of this report, since May 2019 Microsoft provides a lot of public documentation about the Office diagnostic data, especially the data collected with the telemetry client in the Office 365 ProPlus software. The information is written in a technical language, aimed at administrators. It is up to the government organisations to adequately inform their employees.

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.

First of all, data subjects can use the Data Viewer Tool that has been made available since May 2019 by Microsoft to access the telemetry data from Office 365 ProPlus. Alternatively, they can ask their admins to regularly inspect these data, and compare the results with Microsoft's public documentation.

As data processor, Microsoft provides a tool for all data controllers to search and export all data that Microsoft considers to be personal data about a user. This tool is the Data Subject Request tool (hereinafter: DSR).[194] Microsoft has explained that the company will include data from server generated system logs in the output of a Data Subject Request if they are personal data.[195]

In the first Office 365 ProPlus DPIA report for SLM Rijk, Privacy Company has used the DSR tool provided by Microsoft. The obtained files provided information about the use of (cloud-only) Office 365. The files included the first 150 characters of documents that are stored in SharePoint, as a result of the query that Microsoft performs at that moment to find all available content for a user. The DSR file also searches in the SharePoint back-ups, and is able to produce content from documents that were soft-deleted by the user up to 90 days ago. The DSR files do not provide personal data contained in telemetry data or system generated event logs from for example Connected Experiences.

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.

[194] Guidance is available at https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365
[195] See footnote 6, first Office ProPlus DPIA report, 7 November 2018, with reference to Meeting report 28 August 2018, answer to Q2.

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 Exchange Online, SharePoint Online en OneDrive for Business.[196]

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 Data Viewer Tool, via the administrators, via the DSR and the audit logfiles. That a processor redirects requests of the data subject to the controller is in line with the system of the GDPR, but Microsoft should also provide access to the system generated logs created by the use of its processor Connected Experiences.

If a government organisation does not prohibit the use of the Controller Connected Experiences, employees should file a separate data subject request to Microsoft (as joint data controller) to obtain access to personal data collected through the use of these services. Microsoft engages to "*comply with reasonable requests by Customer to assist with Customer's response to such a data subject request*."[197]

Right of rectification and erasure

In the third place, the data subject has the right to have incorrect or outdated information corrected, to have incomplete information completed, and under certain circumstances to have personal information deleted or to restrict processing of personal data. Currently, nor Microsoft nor the government organisations can actually delete historical diagnostic data, except for completely deleting the user account.

Though Microsoft plans to add a more granular delete option to the DSR tool, this would only apply to the data Microsoft recognises as personal data. As explained above, this overview is incomplete. 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.[198] 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.[199]
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).

[196] 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.*"
[197] OST May 2019, p. 8.
[198] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, Answer Q4d.
[199] Ibid, Answer Q4e.

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 365 ProPlus, the processor Connected Experiences 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 would show or withhold 'relevant offers' or targeted advertising to an individual based on the diagnostic data from 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.

Right to data portability

Employees also have a right to data portability, if their personal data are processed based on the necessity to execute the (labour)contract. As outlined in the table in paragraph 11 of this report, the data processing for the three authorised purposes can be based on this legal ground, namely, providing the service, incl. 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.[200]

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.*"

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

[200] 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. This part starts with an overall identification of the risks in relation to the rights and freedoms of data subjects, as a result of 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.

16. Risks

16.1 Identification of Risks

The risks resulting from the storage of diagnostic data can be divided in two categories: metadata and content.

16.1.1 Metadata

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

These contractual improvements prevent Microsoft from using the data to distil a picture/create a profile of a person. However, government organisations can overrule this agreement by explicitly allowing Microsoft to analyse the data. This is the case with the services Workplace Analytics and Activity Reports in the Microsoft 365 admin center, and if the government organisations allow employees to use MyAnalytics and Delve. Similarly, when a government organisation exercises a DSR request, or requests an audit log of the activities of a specific employee, these count as instructions to Microsoft to process the personal data for a profiling or an analytical purpose.

Based on the diagnostic data collected from the end-user devices, Microsoft is able to create detailed information about individual work behaviour, ranging from active time spent on an application, to the detailed statistics about number of words, characters, pictures and paragraphs in a document. If government organisations allow Microsoft to create such analytics by using these services, the employees may experience a chilling effect as a result of the continuous monitoring of their behavioural data. Their employer can use these tools to reconstruct a pattern of effective working hours, from first log-in to last log-out, and time spent with the different applications.

With MyAnalytics employees may feel surveilled in their email behaviour, as senders can see whether they have ‘read’ (opened) an e-mail from the sender. The audit logs show detailed patterns of e-mail behaviour per user, with the subject lines of the e-mails, senders and recipients of e-mail, and minute behavioural details such as the opening, reading, moving and soft or hard deletion of an e-mail. The employer can use this information for a negative performance assessment. Unless the access to these data within the organisation is strictly limited, and logged, and rules are enforced with strong protections such as a four eye access policy, there may be a risk of blackmailing and stalking for the employees.

In sum, Microsoft enables government organisations to perform detailed analyses of individual work behaviour. This may result in a chilling effect on the fundamental rights of employees. They may feel unable to exercise their right to (moderately) make use of government facilities without being observed, to communicate about private affairs, such as sending an e-mail to a friend or family member.

The knowledge that an employer has been, and is, monitoring daily work behaviour may lead to slight embarrassment, shame, and/or change to oral communication, instead of written communication. The feeling of being observed fosters a culture of secrecy. This is a long term risk for government, as such a culture undermines the core values of accountability and open government.

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."[201]

Article 6 of the current ePrivacy Directive obliges all providers to erase or make anonymous metadata when no longer required for the transmission of a communication. Though this rule does not yet technically apply to Microsoft's monitoring of diagnostic data, the principle will be extended to other providers of communication services such as Microsoft in the new ePrivacy Regulation. The storage of metadata over time makes it possible to establish a profile of the individuals concerned, and such information is no less sensitive, having regard to the right to privacy, than the actual content of communications.

The European Court of Justice has explained clearly in its Tele2/Watson ruling why metadata are as sensitive as content data:
"99 That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 27). In particular, that data provides the means, as observed by the Advocate General in points 253, 254 and 257 to 259 of his Opinion, of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."[202]

The data protection authorities confirm in the same vein:" *The risk is not limited to the analysis of the content of communications. Thus, the analysis of metadata about*

[201] Article 29 Working Party (now: EDPB), WP 249, Opinion 2/2017 on data processing at work, p. 9-10.
[202] European Court of Justice, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB (C-203/15) v Post- och telestyrelsen, and Secretary of State for the Home Department (C-698/15) v Tom Watson, Peter Brice, Geoffrey Lewis, ECLI:EU:C:2016:970, 21 December 2016, paragraph 99.

a person might allow for an equally privacy-invasive detailed monitoring of an individual's life and behavioural patterns."[203]

The DPAs also see a risk that employees no longer dare to report anomalies, which can undermine internal whistle-blowing schemes.[204]

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 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. Such a transfer of data from the EU to the USA without a mutual legal assistance treaty as required in Article 48 of the GDPR, would be in breach of confidentiality requirements and the fundamental right to protection of communication secrecy. Such analysis may also breach government secrecy classifications.

Finally, data subjects / citizens that interact with the Government may experience a chilling effect if they know that subject lines from their communication may be stored by Microsoft and further processed by the government organisation outside of the boundaries of the communication with that organisation. For example, in penitentiary facilities, detainees can use Office products such as Outlook. They may be prevented from exercising their right to communicate confidentially with their lawyer if they know the prison has access to metadata disclosing information about this protected communication and there is no clear policy prohibiting further processing.

16.1.2 Content

Microsoft has as a policy that diagnostic data should not include content. In the technical analysis of the telemetry data, no content data were found from documents, emails or conversations, and no directly identifying data such as user names or e-mail addresses. However, the telemetry data do contain locations (URLs and pathnames) of documents, and these may contain personal data. Microsoft also collect snippets of content in system generated event logs, such as the subject line of e-mails, pathnames and titles of documents, but also the contents of documents for which the spelling is checked or of which parts are translated (through the Connected Experiences).

In case of the 14 Controller Connected Experiences, Microsoft may process these data for a variety of purposes that include advertising, product development and product innovation. Microsoft can also use the data for inferred learning, as training sets for machine learning.

Similar to the metadata, there is an additional risk for some types of government employees if the subject lines of emails reveal classified or otherwise government sensitive materials. Additionally, when the organisations use Microsoft cloud storage services such as SharePoint or OneDrive employees may feel unable to exercise their right to (moderately) make use of government facilities to communicate about private affairs, such as opening a file or a financial statement stored in SharePoint.

[203] WP 249, p. 10.
[204] Ibid.

16.2 Assessment of risks

The risks can be regrouped 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 and related rights such as the right to send and receive information)
4. Reidentification of pseudonymised data
5. Unlawful (further) processing

These risks have to 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.

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 currently investigated data processing.

16.2.1 Lack of transparency

Since May 2019 Microsoft provides a lot of public information about the Office 365 telemetry data, and allows users to view the collected data through the Data Viewer Tool. Additionally, data subjects can ask their administrator to perform a data subject access request through Microsofts DSR tool, or create an audit log with activities stored by Microsoft relating to their use of the cloud storage and e-mail services.

Microsoft has not yet published 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). There is a similar lack of transparency about the diagnostic data collected through the Processor and Controller Connected Experiences. 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.

Additionally, Microsoft has not (yet) published any documentation about the diagnostic data collected through Office Online and the mobile Office apps. 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.*"[205]

Given the limited amount of data collected through the telemetry data of Office 365 ProPlus, the possibility to inspect the collected data through the Data Viewer Tool, the possibility to file DSR requests and create audit logfiles, and assuming government organisations follow the recommendation to turn off the Controller Connected Experiences, the impact of the lack of transparency for Office 365 ProPlus is acceptable (even though it could range from minimal to serious), given the agreed purpose limitation.

[205] Ibid.

16.2.2 Lack of control diagnostic data

Since the release of Office 365 ProPlus version 1904, 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.

In view of these controls, and assuming government organisations follow the recommendation to turn off the Controller Connected Experiences, there is little to no change of occurrence of the five major data protection risks described above, while the impact can vary from minimal to serious.

16.2.3 Unlawful processing sensitive metadata and content

The diagnostic data contain sensitive metadata about the individual use of the services and possibly content, through the use of the Connected Experiences. Both types of data may contain highly sensitive or confidential data. As a result of the negotiations, Microsoft will only process personal data for three authorised purposes, regardless of their origin as Customer Data or as diagnostic data or as system-generated server logs.

In view of this purpose limitation, and the effective audit right to verify compliance, assuming government organisations follow the recommendation to turn off the Controller Connected Experiences, the risk of occurrence of harm is minimal. The impact of the processing of the system generated logs for unauthorised purposes could be high, it could lead to serious harm for employees.

16.2.4 Microsoft does not act as a data processor for the Controller Connected Experiences

Prior to the negotiations between Microsoft and SLM Rijk, Microsoft could not be qualified as a data processor, because data processors are legally prohibited from determining the purposes of the data processing. Currently, Microsoft only behaves as a data controller for the 14 Controller Connected Experiences.

Assuming government organisations follow the recommendation to turn off the Controller Connected Experiences, Microsoft only processes the diagnostic data from Office 365 for the three authorised purposes. In combination with the commitment from the Dutch government to audit compliance, there is no risk of unlawful processing of data of employees and other data subjects for unauthorised purposes, and thus, no impact on data subjects.

16.2.5 No effective audit rights and control over sub-processors

Even though Microsoft has attached quite some safeguards to the use of sub-processors, it was difficult -if not impossible- for SLM Rijk and the individual government organisations that use Office 365 ProPlus to verify the integrity of these sub-processors. Similarly, the government organisations did not have effective audit rights to verify compliance with contractual agreements, such as the processing of personal diagnostic data in Cosmos. The audits organised by Microsoft on the data outside of Customer Data are ISO audits. They examine the structure of rules and the existence of checks, but not how the data are factually processed.[206]

[206] For example, Microsoft states an ISO audit has been performed on Cosmos by an independent auditor on the requirements set forth in ISO 27001, ISO 27002 and ISO 27018. However, such ISO audits do not cover the specific risks mentioned in this DPIA, because it only provides a verification of the existence of rules and policies, but does not involve verification of the content of the collected data. Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q10b.

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. The Dutch government has committed in a letter sent on 1 July 2019 to members of parliament to conduct annual audits to verify compliance and publish the summaries of findings.[207]

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.[208] Microsoft has since committed to work on increased transparency of the contracts.

Given the effective audit rights and the commitment of the Dutch government to exercise this right, and assuming government organisations follow the recommendation to turn off the Controller Connected Experiences, the likelihood of occurrence of data protection risks must be assessed as remote, while the possible harm could be qualified from minimal to serious.

16.2.6 Employee monitoring system: chilling effect employees

If government organisations start to deploy Office ProPlus 365 in combination with the (processor) Connected Experiences, and use of 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 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.[209]

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 whistle-blower 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.

---

[207] URL: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019Z13829&did=2019D28465

[208] Meeting report 30 August 2018, answer to Q41.

[209] 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 .

Though the contents of the diagnostic data about the use of Office 365 ProPlus are relatively innocent, the impact for data subjects of unlawful processing of these personal data can be high. Similarly, unlawful processing, or unauthorised reidentification of the pseudonymised diagnostic data from the Connected Experiences and the cloud services can have a high impact on data subjects.

However, the chance that these risks 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. Therefore this results in a low data protection risk.

16.2.7 Lack of purpose limitation Controller Connected Experiences

Prior to the negotiations between Microsoft and SLM Rijk, Microsoft processed the diagnostic data from the Office applications and the Connected Experiences for eight purposes, including all other purposes that Microsoft deemed compatible with those purposes.

As outlined in paragraphs 4.1 and 13, as a result of the negotiations with SLM Rijk, Microsoft has committed to only process the diagnostic data for three authorised purposes, and only where proportionate.

The only remaining risks of further processing by Microsoft for unauthorised purposes relate to the processing of diagnostic data from the Controller Connected Experiences. Assuming government organisations follow the recommendation to turn off the Controller Connected Experiences, the likelihood of occurrence of this risk is 0%, while the severity of the impact depends on the content of the diagnostic data, and can vary between minimal impact to serious harm.

16.2.8 Long retention period

The Office telemetry data are stored for 30 days up to 18 months in the central Cosmos database in the USA. The other diagnostic data are stored between 30 and 180 days.

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

The long retention period of the data in itself poses a data protection risk. However, in view of the agreed and verifiable purpose limitation, the limited amount of data as shown by the telemetry analysis, and the fact that no direct identifiers were observed, or content from documents, the risks of unlawful processing or reidentification of pseudonymised data is remote, while the impact can vary between minimal impact to serious harm.

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.[210]

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

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 365 ProPlus, the processor Connected Experiences and the cloud storage and e-mail services to the United States as data processor with the EU Standard Contractual Clauses. Personal diagnostic data from the Controller Connected Experiences are transferred under the terms of the EU-US Privacy Shield Framework. Microsoft has self-certified under this regime.[211] 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 brought to light by whistle blower Edward Snowden, including the risk of data being observed in transit to the USA.[212]

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.

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

[212] 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. 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.

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.[213] 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.*"[214]

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).[215]

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.

The technical analysis of the telemetry data of the diagnostic data from Office 365 ProPlus shows that Microsoft collects a limited amount of information which does not include snippets of content or direct identifiers. However, because Microsoft qualifies itself as data controller for the personal data from the Controller Connected Experiences, the company makes no commitments to redirect law enforcement requests to the customer. In its 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.*"[216]

---

[213] 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/.

[214] Microsoft OST, June 2019.

[215] 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.

[216] Microsoft general privacy statement, last updated June 2019.

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 the transfer of data from the EEA to the USA, including the level of protection that should be guaranteed during the transit, 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 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 Office 365 ProPlus 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 low risks

These circumstances and considerations as explained above lead to the following eight low data protection risks for data subjects resulting from the diagnostic data processing in Office 365 ProPlus:

1. Lack of transparency: inability to exercise data subject rights and unlawful (further) processing
2. Lack of control diagnostic data: loss of control, unlawful (further) processing
3. Unlawful collection and storage of sensitive data: loss of confidentiality, inability to exercise data subject rights, loss of control
4. Microsoft does not act as a data processor for the Controller Connected Experiences: loss of control, inability to exercise data subject rights and unlawful (further) processing
5. Lack of purpose limitation: unlawful further processing, reidentification of pseudonymised data
6. No effective audit rights and no control over sub-processors: loss of control
7. Employee monitoring system: chilling effect
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:[217]

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

[217] Copied from the DPIA guidance from the UK data protection commission, the ICO. URL: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-carry-out-a-dpia/

Part D. Description of risk mitigating measures

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

The mitigating measures taken by Microsoft have already been discussed throughout the report. As a result, there are no known remaining high risks. The following paragraph contains a table of the eight high risks identified in the first Office 365 ProPlus DPIA for SLM Rijk, and the mitigating technical, organisational and legal measures taken by Microsoft. With regard to the remaining low data protection risks, this paragraph also provides recommendations to government organisations to take additional measures, and to perform DPIAs on the use of diagnostic data for specific analytical services.

17. Risk mitigating measures

17.1 Measures implemented by Microsoft

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.

Since May 2019, Microsoft has published extensive documentation about the Office ProPlus telemetry data. Microsoft has also modified the data viewer tool for Windows 10 telemetry events to also show the Office 365 ProPlus telemetry events. This allows users to see the decoded Office telemetry data Microsoft collects. Since version 1904, released 29 April 2019, Microsoft has also introduced telemetry settings for administrators to be able to determine the desired level of telemetry. Microsoft provides three options: Required, Optional and Neither.

Microsoft has also changed its role and purposes of the processing for many of the Connected Experiences (online microservices). Microsoft is now a data processor for most services that analyse and download content from Office 365, such as the spelling checker (Editor), Translator, and Office Help. Microsoft allows administrators of Office ProPlus to centrally turn off the Controller Connected Experiences. This prevents the risk that employees are shown a question to provide consent for these services, while consent is not a valid legal ground for this data processing.

As a data processor for Office 365 ProPlus, most of the Connected Experiences and cloud storage 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-data and (3) secure.

This strict purpose limitation applies to both the content (Customer Data) and to all diagnostic data, including the system-generated server logs. Microsoft has additionally guaranteed that it won't use the content data or the diagnostic data for the purposes of profiling, data analytics, market research or advertising, unless the customer explicitly requests Microsoft to do so.

The Dutch government has also obtained effective audit rights, and has committed to have an independent auditor perform an annual audit to verify compliance with these measures.

No.	High Risk	Measures taken by Microsoft
1	Lack of transparency	Public documentation and data viewer tool
2	No possibility for administrators to influence the collection of telemetry data	Since Dec 2018: temporary settings to minimise the processing
		Since release of version 1904: admin choices for telemetry levels
3	Unlawful collection and storage of sensitive or classified categories of data through Connected Experiences and diagnostic data on cloud servers with for example filenames	Contractual purpose limitation: processing only for three purposes for which the government organisations have a legal ground
		Microsoft is a data processor for most Connected Experiences + central opt-out from Controller Connected Experiences
		Microsoft will not use content or diagnostic data for profiling, data analytics, market research or advertising
4	Incorrect qualification Microsoft as data processor	Contractual purpose limitation
		Microsoft is a data processor for most Connected Experiences + central opt-out
5	Not enough control over sub-processors and factual processing	Effective audit rights for the Dutch government to have an annual audit performed + commitment to conduct audit and publish summary of findings
6	Lack of purpose limitation	Contractual purpose limitation
7	Employee monitoring system: chilling effect	-
8	Long retention period of diagnostic data	Microsoft is a data processor for most Connected Experiences + central opt-out
		Contractual purpose limitation
		Limitation of future telemetry through switch
9	Transfer of data to the USA	Limitation of telemetry through switch + effective audit rights + contractual purpose limitation. See the paragraphs 7 and 16.8.2 for measures that should be taken by the European Commission

17.2 Measures government organisations

To mitigate the remaining data protection risks, government organisations can also take some measures themselves.

The recommended measures are:

1. Centrally prohibit the use of the Controller Connected Experiences;

2. Upgrade to version 1905 or higher of Office 365 ProPlus and set the telemetry level to 'Neither'. At the level 'Required' Microsoft collects slightly more sensitive data: the organisation needs to ensure that this data processing does not lead to a chilling effect amongst employees;
3. Set the telemetry level in Windows 10 Enterprise to 'Security' (or block telemetry traffic) and do not allow users to synchronise activities via the Timeline functionality. At higher levels, Windows telemetry also collects information about the use of Office ProPlus applications;
4. Disable sending of data for Customer Experience Improvement Program
5. Turn off Linked-In integration with Microsoft employee work accounts;
6. Conduct a DPIA before using Workplace Analytics and Activity Reports in the Microsoft 365 admin center and before allowing employees to use MyAnalytics and Delve;
7. Depending on the sensitivity of the content data: consider using Customer Lockbox and Customer Key;
8. Warn employees not to use Office Online and the mobile Office apps that are included in the Office 365 license until the five high risks have been mitigated.

It follows from the separate DPIA on the diagnostic data collected through Office Online and the mobile Office apps that there are five high data protection risks. These risks result from the fact that Microsoft is a data controller for the mobile Office apps, and allows itself to use the data for all 14 purposes from its Privacy Statement. During the DPIA, traffic has been observed from two Office apps on iOS to a marketing company in the USA. The risks are also a consequence of the fact that Microsoft does not offer a central opt-out for the Controller Connected Experiences in Office Online and the mobile Office apps. Until Microsoft takes measures to mitigate these risks, government organisations should refrain from using Office Online and the mobile Office apps included in Office 365 license.

Last but not least, in order to prevent continued vendor lock-in, government organisations are advised to conduct a pilot with alternative open source productivity software. This would be in line with the government policy to promote open standards and open source software.[218]

Conclusions

As described in the letter sent on 1 July 2019 by the minister of Justice and Security and the minister of Interior Affairs and Kingdom Relation to members of parliament[219], Microsoft and the Dutch government have managed, through a combination of technical, contractual and organisational measures, to mitigate the eight high data protection risks from the first DPIA. If the government administrators take the recommended measures in this DPIA, as a result of the contractual and technical improvements there are no more known high data protection risks for data subjects related to the collection of data about the use of Microsoft Office 365 ProPlus.

[218] Kamerstukken II, 2010-2011, 32 679, Open standaarden en opensourcesoftware bij de rijksoverheid.

[219] URL: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019Z13829&did=2019D28465