DPIA DIAGNOSTIC DATA IN MICROSOFT OFFICE PROPLUS

5 November 2018

Commissioned by the Ministry of Justice and Security for the benefit of SLM Rijk (Strategic Vendor Management Microsoft Dutch Government)

Sjoera Nas
Arnold Roosendaal

Contents

Summary

The Dutch government has commissioned a general data protection impact assessment on the processing of data about the use of the Microsoft Office software. The purpose of this DPIA is to help the individual government organisations map and assess the data protection risks for data subjects caused by this data processing, and to ensure adequate safeguards to prevent or at least mitigate these risks. This report provides a snapshot of the current risks. As Microsoft will provide more information, and more research can be done to inspect the diagnostic data, new versions of this DPIA will be drafted.

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 / OneDrive cloud storage facilities, this DPIA also includes the data Microsoft processes about the use of SharePoint to store and access documents.

Federal negotiations versus individual DPIAs

The Dutch government has a Microsoft Strategic Vendor Management office (SLM Rijk). This office conducts the negotiations with Microsoft for the federal government, but the individual 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 software, including the use of Connected Services. These metadata (about the use of the services and software) are called 'diagnostic data' in this report. This includes so called 'telemetry data'.

Following the logic of ePrivacy legislation in Europe, this report distinguishes between 3 categories of data:

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.

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 3 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. 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 only refers to the specific telemetry data collected through Office itself about the use of the Office software. Microsoft does not have a overall category for the metadata that are generated on its servers by the individual use of the services and software, such as the telemetry data and other metadata stored in server logs. Microsoft uses the term 'Customer Data' to refer to all data that are provided by users when using the software. Most of Microsoft's contractual privacy guarantees relate to these 'Customer Data'.

Data collection via event logs and telemetry

Technically, Microsoft Corporation collects diagnostic data in different ways, via system-generated event logs 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. After an investigation by several European DPAs in 2016-17, Microsoft has published extensive documentation about the Windows telemetry data. Microsoft has also made a data viewer tool available within Windows that allows users to see the telemetry data Microsoft collects. Microsoft has explained that it collects Office telemetry data on a much larger scale (up to 25.000 event types, compared to the max 1.200 event types in Windows 10 telemetry). Within Microsoft, the Office telemetry data are added and analysed by a higher number of engineering teams (20 to 30 teams, compared with the 10 teams that work on Windows telemetry).

Personal data

Currently, Microsoft provides no documentation, settings or data viewer tool for the Office telemetry data. Prior to this DPIA, Microsoft assumed the telemetry data were not personal data As a result of this DPIA, Microsoft recognises that many diagnostic data about the use of the Office software and connected services, including the telemetry data, contain personal data.

The technical administrators of the Office Enterprise software at the different government organisations (the *admins*) can see some system-generated event data if they export the audit log. For the purpose of this DPIA, tests were performed by the technical lab of the Ministry of Justice and Security. The exported audit logs from these tests show that the diagnostic data may include both behavioural metadata and data relating to filenames, file path and e-mail subject lines.

Roles and purposes

Microsoft considers itself to be a data processor for the processing of most of the data it processes through Office, including the Office telemetry data. The only exception is the use of voluntary Connected Services. In that case, Microsoft considers itself to be a data controller, and

may process the diagnostic data for the 12 different purposes described in its general privacy statement that are not excluded in the Online Service Terms.

As a data processor, Microsoft processes the personal diagnostic data 'to provide Office'. This covers processing for the following purposes:

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)
4. Product development (learning to add new features)
5. Product innovation (business intelligence, develop new services)
6. General inferences based on long-term analysis, support machine learning
7. Showing targeted recommendations on screen to the user
8. Purposes Microsoft deems compatible with any these 7 purposes.

Only data controllers may determine the purposes of the processing. In view of the nature of the data processing as examined in this DPIA, Microsoft does not act as a data processor, but as a data controller. Because government organisations enable Microsoft to process personal data for these purposes, the organisations are joint controllers with Microsoft.

The government offers employees no choice in using the Microsoft Office tools. They are not free to select other tools. Employees cannot distinguish between voluntary and mandatory Connected Services and the implications of providing data to Microsoft as an independent data controller. That is why the government organisations and Microsoft are also joint controllers for these discretionary Connected services.

Legal grounds

As joint data controllers, Microsoft and the government organisations can only appeal to 3 of the 6 possible legal grounds. Based on the necessity to perform a contract, including the employment contract, as well as the necessity for a legitimate interest, government organisations may allow Microsoft to process personal diagnostic data for the first three purposes (security, providing updates and troubleshooting). The government organisations can also rely on their legal obligation to process audit logs for security purposes. This can be necessary to collect evidence of possible security breaches as a legal ground for the processing of personal data. Currently, nor Microsoft nor the government organisations have a legal ground for the processing of diagnostic data for any other purpose.

Risks

Currently, Microsoft provides no comprehensive documentation, settings or data viewer tool for an accurate overview of the Office telemetry data. There is limited documentation about the audit logs and system-generated event logs, but no information about the (collection and contents of) telemetry data. New telemetry events, that collect other types of data, can be added dynamically, if they comply with any of the 8 purposes described above.

It is not clear what types of content may be included in the diagnostic data. Microsoft has assured that the audit logs do not contain any part of email content, but the logs do contain the subject lines of emails. Microsoft has also stated that telemetry data may not contain sensitive data or other content, but has simultaneously explained that engineers may have mistakenly added events that could include content. Additionally, snippets of content (such as the line preceding and following a word) may be included in system generated event logs about the use of Connected Services.

Until further examination of the diagnostic data proves otherwise, this report assumes that diagnostic data may include both metadata (about the behaviour of users) and content.

Microsoft does not accept its role as joint controller for the diagnostic data with the government organisations that use Office. The Office telemetry data and system-generated event logs are stored for a minimum of 30 days, and long term for a period of 18 months in the central Cosmos database in the USA. The data can be stored longer if an individual team has exported its own subset of data. There is no central possibility for admins to delete historical diagnostic data, except for terminating the user account. Microsoft has developed rules for the collection of *new* telemetry events, but there was no scheme governing the purposes for the addition of telemetry data in the past. Though Microsoft stores some specific types of Customer Data in European data centres, diagnostic data may be processed and stored anywhere. If an employee uses a voluntary Connected Service, Microsoft may process the data for 12 broad purposes.

These circumstances lead to the following data protection risks:

1. No overview of the specific risks for individual organisations due to the lack of transparency (no data viewer tool, no public documentation)
2. No possibility to influence or end the collection of diagnostic data (no settings for telemetry levels)
3. The unlawful storage of sensitive/classified/special categories of data, both in metadata and in content, such as for example subject lines of e-mails
4. The incorrect qualification of Microsoft as a data processor, in stead of a joint controller as defined in article 26 of the GDPR
5. Not enough control over sub-processors and factual processing
6. The lack of purpose limitation both for the processing of historically collected diagnostic data and the possibility to dynamically add new events
7. The transfer of (all kinds of) diagnostic data outside of the EEA, while the current legal ground is the Privacy Shield and the validity of this agreement is subject of a procedure at the European Court of Justice
8. The indefinite retention period of diagnostic data and the lack of a tool to delete historical diagnostical data

Risk mitigating measures

Microsoft has committed to publish documentation about the Office telemetry data and to offer new telemetry choices for Office admins. Microsoft has also committed to develop a data viewer tool in Office for the Office telemetry data. The timing of these measures is not public information.

In the interim, Microsoft has helped the Dutch government to implement settings to minimise the processing of telemetry data, based on the blocking of traffic from certain ports that send information to the telemetry end-point in the USA. The effectivity of this solution still has to be tested in combination with a data viewer tool. Microsoft and SLM Rijk are negotiating about the use of a data viewer tool. The results of this inspection will be the subject of a follow-up DPIA.

Residual risks

Some residual risks can be mitigated if the government organisations will use the newly developed settings to minimise the processing of telemetry data.
Assuming Microsoft will be offering a data viewing tool and assuming Microsoft will provide global solutions to the risks of the lack of transparency and ability to control the level of telemetry collection, the first two risks will be mitigated by the measures Microsoft has currently committed to take. **Microsoft has not agreed yet to any of the other possible risk mitigating measures**.

Government organisations must exert every effort to mitigate the remaining high risks, amongst others by centrally prohibiting the use of the voluntary Connected Services. They must also block the option for users to send personal data to Microsoft to 'improve Office'. Government organisations should also refrain from using the SharePoint/OneDrive online storage, and delay switching to the web-only version of Office 365 until Microsoft has provided adequate guarantees with regard to the types of personal data and purposes of the processing.

Additionally, the *tenants* should consider the following measures:

- delete some specific users such as VIPs and create new AD accounts for them
- consider using a stand-alone deployment without Microsoft account for confidential/sensitive data
- conduct a pilot with alternative software, after having conducted a DPIA on that specific processing

SLM Rijk should continue to work with Microsoft to obtain further information and conduct follow up DPIA's on future Office versions that may lead to a different appreciation of the data protection risks.

The risks and possible risk mitigating measures can be visualised in the following table.

Nr	Risk	Possible measure Microsoft	Possible measure per tenant
1	Lack of transparency	Public documentation and data viewer tool	Use tool when it becomes available
2	No possibility to influence or end the collection of telemetry data	a. Temporary settings to minimise the processing	Use temporary minimisation settings
			Do not use SharePoint/OneDrive
			Do not use web-only Office 365
		b. Permanent settings for telemetry levels	Use setting telemetry Off when switch is available

3	Unlawful collection and storage of sensitive/ classified/special categories of data	*a. Option to delete historical diagnostic data by Device ID*	Consider deleting some specific users and creating new accounts for them
		b. Guarantee never to store content data in telemetry data or in other system-generated event logs unless strictly necessary	Prohibit users from sending personal data to Microsoft to 'improve' Office
			Consider pilot with other software for some functionality (after conducting a separate DPIA)
4	Incorrect qualification Microsoft as data processor	*a. Minimisation of purposes to be able to act as a processor OR New framework agreement as joint controller*	Endorse new framework agreement as processor or joint controller
		b. Only process data from voluntary Connected Services as a data processor OR change default for voluntary Connected Services to 'Off'	Prohibit voluntary Connected Services unless Microsoft offers these services as a processor
5	Not enough control over sub-processors and factual processing	*More audit rights*	Consider stand-alone deployment without Microsoft account for confidential/sensitive data
6	The lack of purpose limitation	*Processing only for strictly necessary purposes for which the tenants have a legal ground*	- no specific measure, see above
7	The transfer of data outside of the EEA	*New contractual guarantees and/or storage of diagnostic data within the EU*	- no specific measure, see above
8	The indefinite retention period of diagnostic data	*Determine necessary retention periods*	- no specific measure, see above

Given the ongoing negotiations with Microsoft (and Microsoft's written commitments as a part of these negotiations) to mitigate the remaining risks, SLM Rijk postpones consultation of the Dutch data protection authority for risks 3 - 8.

Introduction

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.

This DPIA is focussed on the processing of personal data via diagnostic data generated during the installation and use of Microsoft Office ProPlus software (installed locally, on the device of the users, in combination with online Office 365 services). This DPIA follows the structure of the DPIA Model mandatory for the Dutch government.[1]

Federal negotiations versus individual DPIAs

The Dutch government has a Microsoft supply management office (SLM Rijk). This office conducts the negotiations for the federal government, but the individual organisations buy the licenses and determine the settings and scope of the processing by Microsoft Corporation in the USA. Therefore this general DPIA does not replace the specific risk assessments the different procuring organisations must make, based on their specific deployment, the level of confidentiality of their work and personal data they process.

Definition diagnostic data

This report addresses the data protection risks of the storing by Microsoft of data about the individual use of the Office software, including the use of Connected Services. These metadata (about the use of the services and software) are called 'diagnostic data' in this report. This includes so called 'telemetry data'.

Following the logic of ePrivacy legislation in Europe, this report distinguishes between 3 categories of data:

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.

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

[1] *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.

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 3 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.[2] 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 only refers to the specific telemetry data collected through Office itself about the use of the Office software. Microsoft does not have a overall category for the metadata that are generated on its servers by the individual use of the services and software, such as the telemetry data and other metadata stored in server logs. Microsoft uses the term 'Customer Data' to refer to all data that are provided by users when using the software. Most of Microsoft's contractual privacy guarantees relate to these 'Customer Data'. 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*.[3]

The definition of diagnostic data used in this report is independent from the legal role of Microsoft as a data processor or a data controller.

Previous DPIA on Windows 10 telemetry

The Ministry of Justice and Security in the Netherlands has a separate Microsoft supply management office. This office (SLM Rijk[4]) procures the Microsoft software for all employees of the federal Dutch government. In the spring of 2018, SLM Rijk commissioned a DPIA report about the telemetry or diagnostic dataflow from both Windows 10 Enterprise and the two different Office implementations deployed by Dutch government organisations. SLM Rijk required this analysis as a direct result of the findings of the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, hereinafter: Dutch DPA) that the processing of personal data through Windows 10 telemetry was not compliant with the Dutch data protection act.

This previous DPIA report was written by privacy consultancy firm Privacy Management Partners and delivered in June 2018. The report provides a risk assessment and recommendations to mitigate the data protection risks for Windows 10 Enterprise. The report does not address the specific data processing and risks associated with the collection of data about the use of Microsoft Office software. Within the timeframe set for this initial DPIA, it was not possible to

[2] 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.*"

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

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

obtain sufficiently detailed information about the processing of personal data via Office diagnostic data.

The Dutch DPA and other DPAs in the EU have (as far as publicly known) not investigated the processing of personal data via diagnostic data generated by the use of the Office software. Therefore SLM Rijk has asked the technical lab of the ministry of Justice and Security to analyse the diagnostic dataflows generated in specific scenario's for the four most widely used Office applications, and the use of SharePoint Online to store documents in Microsoft's cloud. SLM Rijk has commissioned Privacy Company to conduct a second DPIA on the diagnostic data generated by the use of the Office software.

Technical limitations

The technical lab was unable to inspect the contents of the outgoing data stream. As an essential security measure, Microsoft encodes the outgoing traffic to its own servers. Microsoft did not provide tools to the lab to decode the outgoing data stream. It was not (yet) possible to view the contents of the traffic in another way, because Microsoft had not yet developed a tool to be able to view the diagnostic data in a way similar to the Data Viewer Tool provided for the Windows 10 telemetry data. However, Privacy Company is working with Microsoft to analyse the collected telemetry data. Microsoft has also offered a test version of a data viewer tool to be teste by SLM Rijk. The analysis of the contents of the diagnostic events will take some time. The lab cannot perform this analysis overnight, and it is likely that further explanations from Microsoft are required. Therefore, this analysis cannot be performed within the agreed time schedule to deliver this DPIA report. This report has therefore to be seen as a first general outline of the data processing risks. After the contents of the diagnostic data have been analysed, it is hopefully possible to quickly conduct a follow-up DPIA.

Meetings with Microsoft

To gain understanding of the data processing and risks, representatives of the Ministry of Justice and Security and representatives of Privacy Company have held a series of meetings with Dutch and American representatives of Microsoft Corporation between 28 August and 3 September 2018. Microsoft has kindly provided oral answers to many detailed questions. Unfortunately, Microsoft has not provided any specific reaction on the detailed meeting reports that were sent to Microsoft one day after every meeting. In spite of repeated commitments to do so, Microsoft also did not provide any formal written answers to the list of 100 questions raised during the meetings. Following the agreed time schedule, parts A and D and the summary of the draft DPIA report were sent to Microsoft on 17 September 2018.

On 24 September 2018, Microsoft has provided a general written response, without any specific comments on (paragraphs in) the report, but with some additional information. Microsoft has indicated that this written information is *authoritative* and thus should replace any statements to the contrary made during the meetings that were included in the draft DPIA. However, Microsoft also indicated that the document was confidential. When asked how to deal with secret but authoritative answers, Microsoft has specified that SLM Rijk may not share the document, but may use the facts. Microsoft has requested not to disclose any time schedules and unpublished product changes. Microsoft has also requested not to be quoted verbatim in this DPIA report if a statement was a mere opinion, and not a fact. These requests have been processed in this report.

After a meeting with SLM Rijk about this DPIA on 28 September 2018, on 1 October 2018 Microsoft has provided brief answers to the list of 10 questions and sub-questions which arose as a result of Microsoft's initial response to this DPIA report. The answers to these questions have also been added to this report, when relevant. Most answers however referred back to the initial response.

Further meetings between Privacy Company and Microsoft were held on 30 October en 1 November 2018. Microsoft provided additional explanations per e-mails of 1 and 2 November 2018.In this DPIA report information from Microsoft is supplemented with publicly available documentation.

Outline

This assessment follows the structure of the *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017).[5] This model uses a structure of four main divisions, 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 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, input from Microsoft has been processed.

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

In Part C the risks for data subjects are assessed, as caused 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 mitigate these risks as well as their impact. Finally, this part also contains an assessment of the residual risk attached to the collection of diagnostic data about the use of the Office software, even after applying measures to mitigate the risks.

[5] 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

This data protection impact assessment was carried out by Privacy Company between August and October of 2018.

Part A. Description of the Office diagnostic data processing

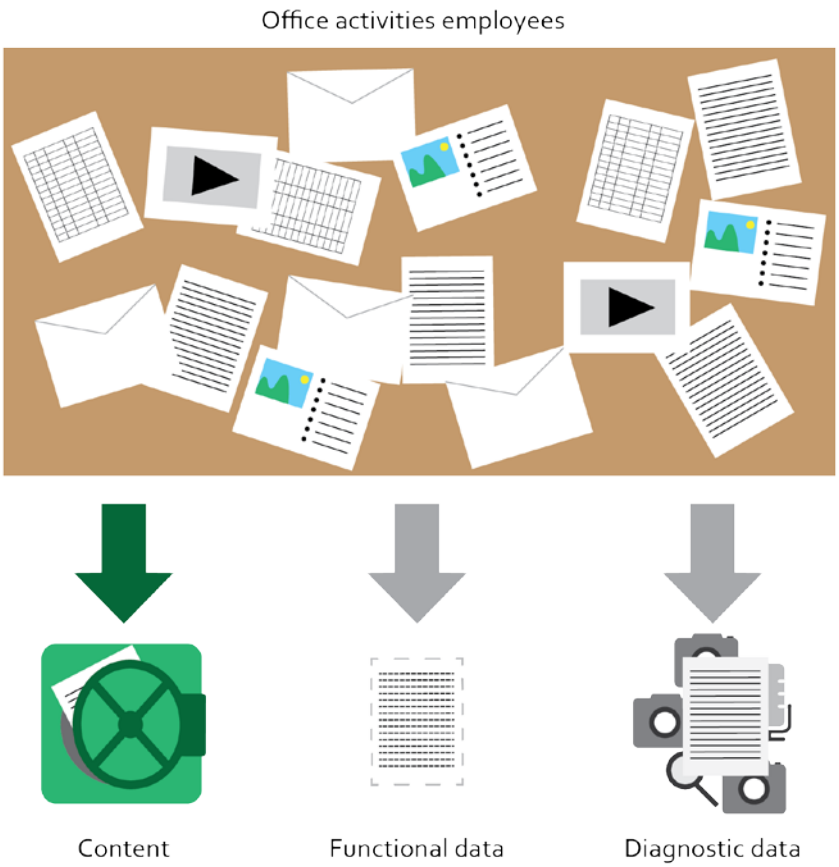
This first part of the DPIA provides a description of the characteristics of the diagnostic data collected via the use of Office software. This starts with a short description of the processing of different kinds of data (content, diagnostic data and functional data).

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. Topic: the processing of diagnostic data in Microsoft Office Software

This DPIA concerns a general overview of some general risks caused by the processing of personal data *about* the use of the Microsoft Office ProPlus software (Office 2016 MST and Office 365 CTR), in combination with Connected Services. 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



As will be explained in more detail below in section 3, *Data processing through 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.

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.[6] The Microsoft Office software is not new. But 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 *tenants* in the Netherlands to conduct a DPIA based on the criteria published by the Dutch data protection authority.[7] The Dutch government Microsoft supply management office (SLM Rijk) conducts the negotiations with Microsoft and manages the government-wide framework for the procurement of the software.

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 has commissioned this DPIA to assist the *tenants* to select a privacy-compliant deployment, and conduct their own DPIA's where necessary.

About Microsoft Office and Connected Services

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.

Connected services are different from the commonly known Office services such as Word or Excel. In the first place, of course, these Connected services are 'connected'. This means that the use of these services is only possible if the application can communicate with the Microsoft servers. Secondly, Connected services are served in 2 flavours: either mandatory, or discretionary (voluntary). In case the use of the Connected service is discretionary, the individual end-user may turn the services on if they wish to use them. 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 section 5 of this DPIA *Roles: Data controller, data processor and sub-processor*, Microsoft considers itself to be a data controller for the use of discretionary Connected Services. Currently, Microsoft offers 31 Connected Services, of which 17 are discretionary.

[6] Source: Microsoft Business and Services Agreement, Amendement ID CTM, May 2017.

[7] 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 vulnerabe 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.

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. A short summary of features and the full list of Connected Services is provided in Annex 1.

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

Scope

The aim of this DPIA is to assess whether and how 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 risks for the privacy of the users may be. Moreover, this report assesses how the identified risks can be mitigated by means of technical and organizational measures. The scope is limited to the processing of diagnostic data by the four main applications provided in Office: Outlook including Calendar functions, Word, Excel and PowerPoint. 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 Services, such as an online spelling checker or dictionary.

Connected services are different from other features that can be used within the main applications. In the current contract between Microsoft and SLM Rijk, the collection of data through some of these Connected Services is excluded from the agreed privacy protections in the Enrolment framework. If the end-user decides to use these services, Microsoft considers that it is a data controller, and may process the resulting personal data for its own purposes, as outlined in the General Privacy Statement. Therefore, this report will distinguish between discretionary and mandatory Connected Services.

Out of scope

This DPIA does not describe the specific deployments chosen by the different government organisations that procure the Office software (see section 8 in the DPIA). In Microsoft terminology, the government organisations are called *tenants*. It is up to these different *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.

Similarly, this DPIA report does not provide an analysis of the data protection risks caused by the use of web-based Office 365 (Microsoft cloud-only environment). First Microsoft and SLM Rijk have to agree on a technical way to investigate what the diagnostic data that Microsoft stores on its own servers. This report describes the storage of documents in SharePoint Online, but no other types of storage in the Microsoft cloud. The Dutch government mainly stores content data in its own data centres (on-premise).

In practice most government employees use 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 *tenants* 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.

Given the short timeframe to conduct this DPIA, other choices had to be made about the scope. This DPIA does not address risks caused by the separate tools Workplace Analytics, Delve and Windows Analytics. This DPIA also does not assess the risks of the combination of Office diagnostic data with LinkedIn diagnostic data. Office software can be used on devices with different operating systems, such as different Windows versions and Apple operating systems (iOS and MacOS). The scope of this report is limited to the processing of personal data via diagnostic data when using the selected Office ProPlus versions on the operating system Windows 10 Enterprise, with the Windows 10 telemetry setting set to the minimum of 'security'. However, this report provides a snapshot of the current risks. As Microsoft will provide more information, and more research can be done to inspect the diagnostic data, new versions of this DPIA will be drafted and the scope may be expanded.

2. Personal data and data subjects

The Dutch government DPIA model requires that this section provides a list of the kinds of personal data that will be processed via the diagnostic data, and per category of data subjects, what kind of personal data will be processed by the product or service for which the DPIA is conducted. In this case, the answer to the question whether Microsoft processes personal data via the diagnostic data, is not obvious, nor neutral, and the answer to the question which personal data will factually be processed via the diagnostic data, is not within the scope of this DPIA.

First, due to the fact that the contents of the diagnostic data could not be inspected, it is not obvious which diagnostic data that Microsoft collects about the use of the Office software are personal data. The lab has only been able to detect (with network monitoring tools) to what endpoints traffic was sent, to what extent the amount of traffic varied per tested scenario, and whether the traffic stream was publicly documented by Microsoft. However, in order to help the *tenants* understand the range of different types of diagnostic data that Microsoft may collect about the use of the office software, Privacy Company has looked at the audit log about the use of the Office software in these test scenario's, and other usage by other people in *real life* circumstances.

Second, Microsoft does not agree with the qualification of all of the diagnostic data as personal data as defined in article 4(1) a of the GDPR. As a result of this DPIA, Microsoft does accept that the diagnostic data may contain personal data.

Microsoft has not provided a comprehensive list of types of diagnostic data that it considers personal data. If diagnostic data are personal data, Microsoft has said it will include those data in the output of a Data Subject Request.[8] The different kinds of data that Microsoft processes, will be described in more detail in section 3 of this DPIA, *Data processing via Office diagnostic data*.

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

Third, this DPIA can only provide general assistance to the actual data controllers, the *tenants*, to assess the kinds of personal data that may be included in diagnostic data, and the kinds of data subjects that may be involved. The actual data processing strongly depends on their privacy choices and settings, and the nature of the work performed by their employees.

These three circumstances will be described in more detail in the three sub sections below.

2.1 Audit logs

Microsoft offers an audit log tool to admins of Office ProPlus Enterprise.[9] Microsoft explains: "*You (or another admin) must turn on audit logging before you can start searching the Office 365 audit log. When audit log search in the Office 365 Security & Compliance Center is turned on, user and admin activity from your organization is recorded in the audit log and retained for 90 days.*"[10] However, Microsoft also notes it is in the process of changing the default: "*We're in the process of turning on auditing by default. Until then, you can turn it on as previously described.*"[11]

The data obtained about the usage of the Office software in the lab reflect a number of standardised activities executed by the lab. In each of the four main functionalities of Office the lab performed a limited set of activities; such as creating and closing a document in Word, Excel and PowerPoint, and opening and storing it in SharePoint Online, as well as sending e-mails in Outlook with different titles and attachments.[12] The Office applications were tested for the two different Office deployments, with different privacy settings. All scenarios were separately combined with the use of some additional Connected services, such as the online spelling checker.

The Audit log contains four main categories of information: CreationDate, UserIDs, Operations and Auditdata.

An example of (obfuscated) AuditData[13]

{"CreationTime":"2018-09-01T10:54:00",
"Id":"5c15b4ec-b197-470b-afe7-04729a3d1f86",
"Operation":"UserLoggedIn",
"OrganizationId":"b61b13fc-e936-4ada-b443-f663048afd59",
"RecordType":15,
"ResultStatus":"Succeeded",
"UserKey":"10033FFF8121346C@[HOSTNAME].nl",

[9] Guidance is available at https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

[10] Microsoft, Turn Office 365 audit log search on or off, URL: https://docs.microsoft.com/en-us/office365/securitycompliance/turn-audit-log-search-on-or-off

[11] Microsoft, Search the audit log, URL: https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

[12] A typical example of such a scenario is:

- Start Microsoft Word
- Select 'empty document' template
- Add text
- Add a local image
- Store the document locally
- Close Microsoft Word

[13] Privacy Company has replaced the directly identifying data by X-s or generic words such as 'hostname'.

"UserType":0,
"Version":1,
"Workload":"AzureActiveDirectory",
"ClientIP":"XX.XXX.XXX.XXX",
"ObjectId": "00000003-0000-0000-c000-000000000000",
"UserId":"[NAME]@[HOSTNAME].nl", "AzureActiveDirectoryEventType":1,
"ExtendedProperties":[{"Name":"UserAgent", "Value":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/64.0.3282.140 Safari\/537.36 Edge\/17.17134"}, {"Name":"UserAuthenticationMethod","Value":"1"},
{"Name":"RequestType","Value":"OAuth2:Authorize"},
{"Name":"ResultStatusDetail","Value":"Redirect"},
{"Name":"KeepMeSignedIn","Value":"True"}],
"Actor":[{"ID":"49cef3de-b42f-4c80-a01a-57e792e9432d",
"Type":0},{"ID": [NAME]@[HOSTNAME].nl,"Type":5}, {"ID":"10033FFF8121346C","Type":3}],
"ActorContextId":"b61b13fc-e936-4ada-b443-f663048afd59",
"ActorIpAddress":"XX.XXX.XXX.XXX",
"InterSystemsId":"17cfaacc-f430-4387-a9ff-811aa2f9b801",
"IntraSystemId":"9ad99199-b734-4714-8198-98b3d6350c00",
"Target":[{"ID":"00000003-0000-0000-c000-000000000000","Type":0}],
"TargetContextId":"b61b13fc-e936-4ada-b443-f663048afd59",
"ApplicationId":"89bee1f7-5e6e-4d8a-9f3d-ecd601259da7"}

Another example of (obfuscated) AuditData:[14]

"CreationTime":"2018-06-04T14:11:30",
"Id":"2d406d82-c282-4be7-a82c-08d5ca2511c8",
"Operation":"FileAccessed",
"OrganizationId":"b61b13fc-e936-4ada-b443 f663048afd59",
"RecordType":6,
"UserKey":"i:0h.f|membership| [xxxxxxxxxxxxxxxx]@live.com",
"UserType":0,
"Version":1,
"Workload":"OneDrive",
"ClientIP":"XX.XXX.XXX.XXX",
"ObjectId":"https:\/\/[HOSTNAME]-my.sharepoint.com\/personal\/[NAME]_[HOSTNAME_nl\/Documents\/Gedeeld met iedereen\/Event 20180607\/PPT 06 Advies SLM.pptx",
"UserId":"[NAME]@[HOSTNAME].nl ",
"CorrelationId":"05d56d9e-a035-5000-b848-4c14733cf7ff",
"EventSource":"SharePoint",
"ItemType":"File",
"ListId":"e3f0c017-6b47-460f-9c8c-42bf9028709c",
"ListItemUniqueId":"8ef4463f-8e04-42d7-a391-5a6e61d9527f",
"Site":"edc7e633-d930-46e5-8364-7da6339e952b",
"UserAgent":"Microsoft Office PowerPoint 2014",
"WebId":"af2a900c-18e2-414e-a8f2-968867f84fb9",
"SourceFileExtension":"pptx",

[14] Privacy Company has replaced the directly identifying data by X-s or generic words such as 'hostname'.

"SiteUrl":"https:\/\/[HOSTNAME]-my.sharepoint.com\/personal\/[NAME]_[HOSTNAME_nl]\/","SourceFileName":"PPT 06 Advies SLM.pptx","SourceRelativeUrl":"Documents\/Gedeeld met iedereen\/Event 20180607"}

The audit log shows when who accessed a document, including all user and admin activities for all services,[15] including the subject line of a message that was accessed from an Exchange server.[16] If (separately) switched on by the admin of the tenant, the audit log may also be searched for all e-mail activity of a user.[17] This includes the following activities: copy, create, softdelete and harddelete, message previewed or opened, moved to delete folder and updateinboxrules.[18]

The examples of the audit log shown above contain directly and indirectly identifying data such as e-mail addresses, names and IP-addresses. In the second example, a private user e-mail address @live.com is combined in the log with the professional e-mailaddress@hostname.nl. These data clearly fall under the definition of personal data. Other types of identifiers included in the audit log, such as Organisation ID, Correlation ID, WebID, InterSystems and IntraSystemID's may be personal data as well, if Microsoft has the ability to combine one or several of these unique identifiers with other data stored by Microsoft as diagnostic data. If one or more of the unique identifiers in an event are personal data, all elements in the event (and possible subsequent events that can be linked to that event, with, for example, a sequential number) have to be qualified as personal data, relating to the behaviour of an individual user.

In response to this DPIA Microsoft has explained that the policy is that the audit logs may not contain any part of file or email content. Microsoft acknowledges that audit logs may contain some Customer Data and Personal Data (such as a person's name, e-mail addresses, file names and file paths), but this is a necessary aspect of security logging. Microsoft has not provided an explanation with regard to the subject line of e-mails (which is a brief summary of the content), other than the reminder that it is up to users and tenants to be careful with the information they share via publicly accessible headers.

Microsoft has also confirmed that audit logs are not part of the (protected category of) Customer Data. Microsoft processes the data in the audit log for the same purposes as Customer Data. Microsoft has specifically denied using the audit logs to create psychometric profiles of natural persons, by combining audit logs with other data.

[15] If 'Show results for all activities' was selected by the admin.
[16] Microsoft, Detailed properties in the audit log: Subject - The subject line of the message that was accessed - Exchange (mailbox activity)
[17] See: Microsoft, Enable mailbox auditing in Office 365, URL: https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing ."*By default, mailbox auditing in Office 365 isn't turned on. That means mailbox auditing events won't appear in the results when you search the Office 365 audit log for mailbox activity. But after you turn on mailbox audit logging for a user mailbox, you can search the audit log for mailbox activity*."
[18] See the table with Mailbox auditing actions, bottom half of the page, URL: https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing.

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.

It is not clear which personal data, including data about the behaviour of the user are and can be included in Office system-generated event logs, and in event logs from the Connected Services, outside of the category of data that Microsoft describes and protects as Customer Data.

In its response to this DPIA report, Microsoft explicitly denies that customer content may be included in the diagnostic data. Microsoft writes 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 writes 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.

Microsoft has also 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 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.*"[19]

However, absent a tool to inspect the telemetry data and system-generated event logs, and absent comprehensive documentation, this statement needs to be verified before it can be taken as a fact.

2.2 Definition of personal data

According to article 4 (1) (a) GDPR,

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

The Dutch DPA concluded in its public investigation report about Windows 10 telemetry data 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.[20] The Dutch DPA explained that when object data are

[19] E-mail Microsoft 4 November 2018.

[20] Dutch DPA, report of findings Microsoft Windows 10, the processing of personal data via telemetry (in Dutch only), p. 101. URL: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_onderzoek_microsoft_windows_10_okt_2017.pdf A summary in English is available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/public_version_dutch_dpa_informal_translation_summary_of_investigation_report.pdf

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.[21] As part of its research, the Dutch DPA filed a data access request for its research accounts and established that it was possible for Microsoft to link the e-mail addresses to the user identifiers, and the user identifiers to device identifiers.[22]

The likelihood of identifiability increases considerably with the ability to link different data events to an individual user. As will be explained in section 8 of this report, the processing of telemetry processing involves large amounts of data, with up to 25.000 different types of events. Microsoft has explained lots of engineering teams can add events to the data stream, while until recently there were no central rules governing the collection of the Office telemetry data.[23]

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.

Just like the Windows 10 telemetry data, the Office telemetry data are stored in the central Cosmos database. Microsoft explains in its own Office 365 GDPR compliance assessment, "*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.*"[24] Microsoft explains that system-generated event logs are stored in Cosmos as well.[25]

In response to this 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 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."*[26]

[21] Idem.
[22] Idem, p. 103.
[23] Meeting report 28 August 2018, answer to Q1. In its response to this DPIA Microsoft has explained that there are rules governing the collection of *new* telemetry events. See section 8 of this DPIA report.
[24] 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.
[25] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q4f.
[26] Microsoft confidential response to this DPIA report, 24 September 2018, p. 21.

According to Microsoft, some (other) diagnostic data may (also) be personal data as defined in the GDPR (and part of the class of data which Microsoft calls Customer Data), but Microsoft has not provided a comprehensive list of types of diagnostic data that it considers personal data. The different kinds of data that Microsoft processes, will be described in more detail in section 3 of this DPIA, *Data processing via Office diagnostic data*.[27]

Anonymisation / pseudonymisation / dehydratation

As will be discussed and illustrated with screenshots in section 4 of this report, *Purposes*, Office 365 users can "*Send personal information to Microsoft to make improvements to Office*."[28] Microsoft publicly assures users that the data it collects if this box is ticked, are anonymous, because only a random identification number is attached to the event data.[29] But this reassurance does not specifically relate to Office diagnostic data. In fact, Microsoft does not provide an explanation what type of diagnostic data are used to 'improve' Office. The new explanation provided in the most recent build of Office 2016 MST explains that Microsoft wants to use content to make product improvements.[30]

Anonymisation is a complex and dynamic process.[31] Very often, organisations still possess original data in other databases, or continue to collect non-anonymised data. But as long as there is a realistic possibility to re-identify the masked data, they cannot be considered anonymous and the organisation still needs a legal ground for the collection of the personal data. In such circumstances, the deletion of directly identifying data, and the storage of data in a hashed format, instead of storing the original data, are good technological measures to protect the confidentiality of the data. Microsoft recognises explicitly in its Online Service Terms that pseudonymised data are personal data. *Pseudonymized identifiers may also be generated through Customer's use of the Online Services and are also Personal Data.*[32] Microsoft has also stated that data which can be 're-hydrated' (re-identified), are not anonymous data.[33] At the same time, in its general privacy statement, Microsoft uses the term de-identified, when describing its use of data to develop new products.[34]

---

[27] The name of the database and its telemetry contents are discussed in a publicly available article that has been co authored by 3 Microsoft engineers. Titus Barik, Robert DeLine, Steven Drucker, Danyel Fisher, The Bones of the System: A Case Study of Logging and Telemetry at Microsoft, May 2016, URL: https://www.microsoft.com/en-us/research/publication/case-the-bones-of-the-system-a-study-of-logging-and-telemetry-at-microsoft/

[28] Text provided in the privacy options for Office 365 CTR Version 1803.

[29] https://support.office.com/en-us/article/view-my-options-and-settings-in-the-microsoft-office-trust-center-d672876e-20d3-4ad3-a178-343d044e05c8. Information last checked 26 September 2018.

[30] The text has changed in the most recent version 1808 of Office 2016 MST, to: "*Get designs, information, recommendations, and services by allowing Office to access and make product improvements based on Office content on my device.*" See section 4 of this report for screenshots.

[31] 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

[32] Microsoft Online Service Terms (OST), version used of 1 September 2018, available via: https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx

[33] Meeting report 28 August 2018, answer to Q10.

[34] Microsoft Privacy Statement, under "How We Use Personal Data", available at: https://privacy.microsoft.com/en-GB/privacystatement. "*We use data to develop new products. For*

Because anonymisation strongly depends on the actual circumstances of the processing, any statement of anonymisation has to be verified technically. 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. The inspection by the Dutch DPA with the data viewer tool showed that with the Windows 10 telemetry, Microsoft collected lines from the content of handwritten texts, in combination with unique identifiers. The fact that Microsoft had taken technical measures to limit the identifiability in storage, such as immediately removing the identifiers, and removing known identifiers such as e-mail addresses, did not change the conclusion that Microsoft was processing personal data, both during the initial storing of the Windows telemetry data on the device and during the sending of the data to Microsoft servers.

Based on the foregoing, while waiting for the analysis of the contents of the diagnostic data, this DPIA assumes that the Office diagnostic data are personal data. This assumption is based on the following circumstances:

1. The fact that Microsoft explains that all audit logs and system-generated event logs are uploaded to its central database Cosmos, and these data may include hashed or encrypted end user identifiable information and what Microsoft calls pseudonymous identifiers;
2. The fact that Windows 10 telemetry data are stored in Cosmos, and are personal data according to the Dutch DPA, in spite of earlier denials of Microsoft;
3. The large scale of the collection of telemetry data (up to 25.000 events, compared to the max 1.200 events in Windows 10 telemetry) – see section 8 of this report;
4. The number of engineering teams with different types of analytical questions and problems to solve (20 to 30 teams, compared with the 10 that work on Windows telemetry) – see section 8 of this report;
5. Until recently, the lack of a central policy governing (and limiting) the collection of event data – see section 8 of this report.

2.3 Possible types of personal data and data subjects

As underlined 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.

Categories of personal data

Generally speaking, users and employers can process all kinds of personal data in Office. These products can be used for many different purposes by many different organisations. Absent a comprehensive documentation and publicly available policy rules governing the types of data that can be stored by Microsoft as diagnostic data, it has to be assumed that Office diagnostic data may include all categories of personal data. Some kinds of data deserve extra attention.

---

example, we use data, often de-identified, to better understand our customers' computing and productivity needs which can shape the development of new products."

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.[35]

Classified Information is not a separate category of data in the GDPR or other legislation concerning personal data. But 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 or OneDrive, 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 server side logs. If the organisation uses an Exchange server, Microsoft may log the subject line.

Sensitive personal data

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

The sensitivity is related to the level of risk for the data subjects in case the confidentiality of the data is breached. Risks may vary between slight embarrassment, shame, a chilling effect preventing a data subject from seeking further assistance from that government organisation or 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.

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

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

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) may be included in system generated event logs about the use of Connected Services.

Special categories of personal data

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

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

With special categories of data, the principle is one of prohibition: special data may in principle *not* be processed. There are exceptions to this rule, however, for instance when the data subject has explicitly consented to the processing, or when data has been made public by the data subject, or when processing is necessary for the data subject to exercise legal claims.[36]

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.

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 3 groups, namely: employees, contact persons and miscellaneous.

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

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

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.

3. Data processing through diagnostic data

As summarised in the introduction and section 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 Services. But what are diagnostic data?

For the purposes of analysis and following the logic of ePrivacy law in Europe, this DPIA uses 3 broad groups of data (content, diagnostic and functional data).

In this report, all data *about the individual use of the Office applications and Connected Services* 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', events about the usage of the software are collected in a client programmed in the software installed on the device that are regularly sent to Microsoft's servers.

The way the telemetry client captures data, is described in section 8 of this report. The purposes for which Microsoft collects diagnostic data are described in the next section of this report.

Microsoft uses different words and classifications. The term 'diagnostic data' for Microsoft only refers to the specific telemetry data collected through Office itself about the use of the Office software. Microsoft does not have a overall category for the metadata that are generated on its servers by the individual use of the services and software, such as the telemetry data and other metadata stored in server logs. According to Microsoft *"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. (…)"[37] Most of Microsoft's contractual privacy guarantees relate to these 'Customer Data'.

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.[38] 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 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. Microsoft protects the security of these personal data outside of the scope Customer Data following the requirements set forth in ISO 27001, ISO 27002, and ISO 27018.[39] Microsoft also collects personal data when providing support to customers.[40]

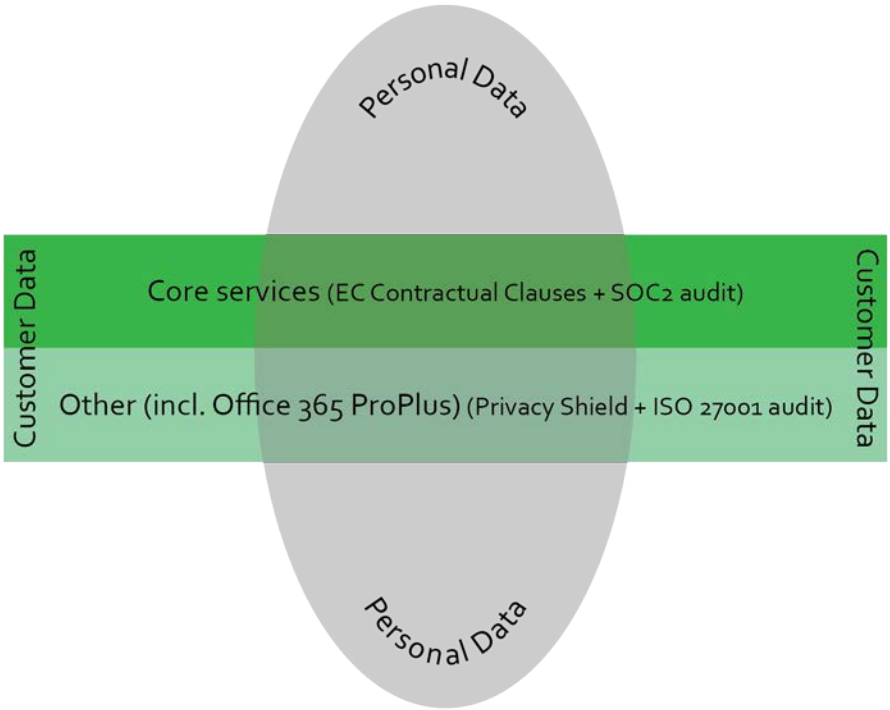
Illustration 2: Microsoft classification of Customer Data and Personal Data

[37] Microsoft Online Service Terms, August 2018, 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. 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*

[38] Microsoft OST:"*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."* (…)

[39] Explanation provided by Microsoft in e-mail of 1 November 2018.

[40] Microsoft collects other kinds of personal data, for example if a customer contacts Customer Service. Microsoft defines Support data in the OST as follows: "*Support Data" means all data, including all text, sound, video, image files, or software, that are provided to Microsoft by or on behalf of Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain technical support for Online Services covered under this agreement.*" The processing of these data is outside the scope of this DPIA.



Telemetry data provide Microsoft with quality information about the functioning of the software. 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."*[41]

A subset of diagnostic data is contained in audit logs. These audit logs (examples provided in section 2 of this report) are created by Microsoft for security purposes, and provide a view for the user to some of 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). The audit logs contain information about for example access to files in SharePoint, or the subject line of an e-mail. To the extent that Microsoft generates audit logs for its internal services (Microsoft's own security logs), these logs are out of the scope of this DPIA. But the audit logs that Microsoft makes available to the admin are within the scope, as they contain information (and likely personal information) about the use of the Office software.[42]

[41] Meeting report 3 September 2018, new question renumber.

[42] Microsoft provides some public information about the Audit logs at: https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance and the subsection https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#audited-activities. Other information is available at https://support.office.com/en-us/article/activity-reports-in-the-office-365-admin-center-0d6dfb17-8582-4172-a9a9-aed79815026 3?ocmsassetID=0d6dfb17-8582-4172-a9a9-aed79815026 3&ui=en-US&rs=en-US&ad=US.

Microsoft has explained that the audit logs do not contain telemetry events.[43] However, both the telemetry and the audit data can be considered a subset of diagnostic data, since they both contain event data about the use of the software.

Some data which are generated by the use of the services are functional data. Microsoft uses a different definition for functional data, namely, only the content data that a user actively sends to Microsoft when using a Connected Service. This report defines functional data in a different way, namely, as, data that have to be transmitted from the user device to communicate with services on the Internet, including Microsoft's own apps and services. Examples of such functional data are the data processed by an e-mail server, and the data stream necessary to allow the user to authenticate or to verify if the user has a valid license. Functional data may also include snapshots that Microsoft collects about the configuration of the Office software in order to provide updates. Functional data may also include the content of a query sent to search engine Bing, or 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.[44] Thus functional data may include content data. The key difference between functional data and diagnostic data is that functional data are and should be transient. 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.

A third category of data is content data, such as documents and pictures that are actively provided to Microsoft by the users of the Office software, for example by using the e-mail client, or storing documents in SharePoint Online or OneDrive for Business. Microsoft defines these data as Customer Data. As will be described in section 8 of this DPIA, the Dutch government stores content data on its own servers, on-premise. However, the Dutch government is currently testing the use of SharePoint online to store documents in the (EU) Microsoft cloud.

As will be described in more detail in section 7 of this report, Microsoft gives the strongest privacy protections to Customer Data provided in Core Services (such as SharePoint, OneDrive, 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 Standard Contractual Clauses.

Customer Data provided through 'Other' services, such as the Office ProPlus 365 software, are audited under ISO 27001, and the transfer is protected by adherence to the (self-certified) Privacy Shield. Microsoft has explained in response to this DPIA report that Customer Data may include content that is sent to Microsoft as a result of using the mandatory Connected Services, when Microsoft considers itself to be a processor (see Annex 1). These privacy protections do not apply to telemetry data, audit logs and system-generated event logs, including the use of the discretionary Connected Services.

None of these sources provide a limitative overview of the types of personal data that Microsoft collects via system-generated event logs.

[43] Meeting report 3 September 2018, answer to Q6.

[44] Meeting report 3 September 2018, p. 1.

3.1 Privacy choices in Office

Government organisations can influence the processing of diagnostic data via a number of settings. The end-users (employees and workers) also have some choices, though many of these choices can be overruled by the admin. The processing of diagnostic data is also 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 section 8 *Techniques and methods of the data processing*.

Users of the Office software can access privacy settings through any of the four main applications, through the Trust Center. Under the tab 'Privacy Options' they can find two options:

- Send personal information to Microsoft to make improvements to Office
- Let Office connect to online services from Microsoft to provide functionality that's relevant to your usage and preferences

In the most recent build of Office 2016, the text for these two options has changed. The options are:

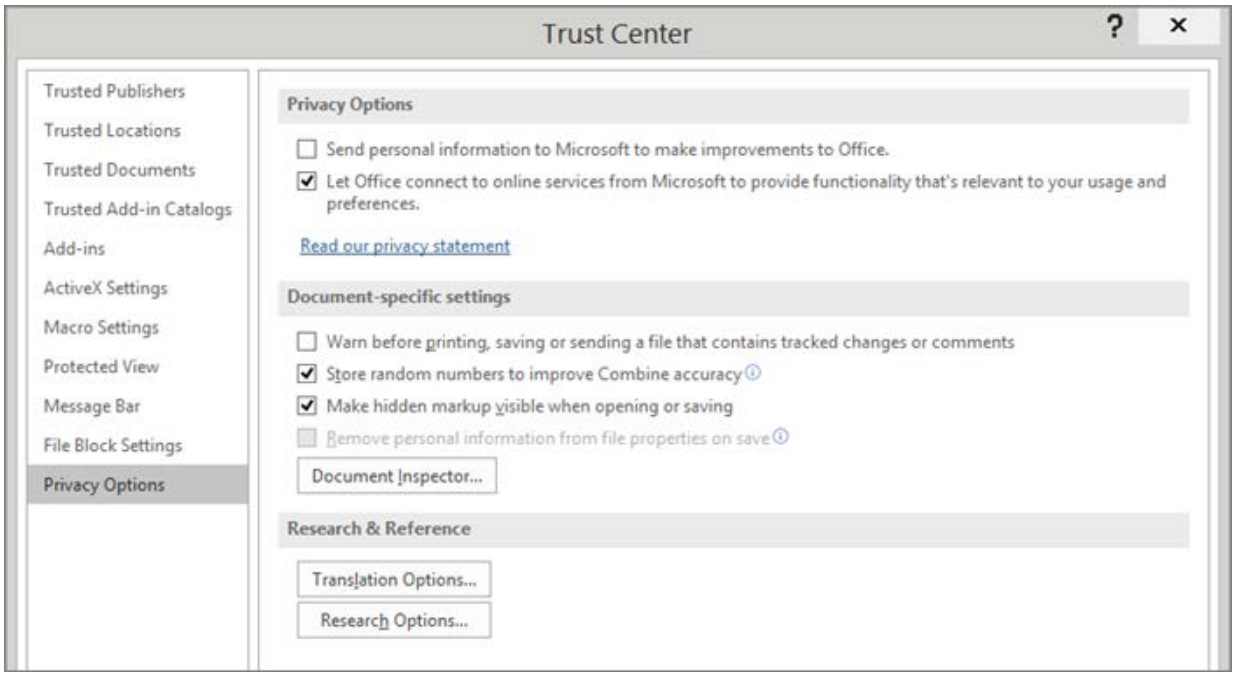
- Get designs, information, recommendations, and services by allowing Office to access and make product improvements based on Office content on my device.
- Let Office connect to online services from Microsoft to provide functionality that's relevant to your usage and preferences.

However, in both cases, by default, the first choice is 'Off', the second choice is 'On'. There is no hyperlink or other reference in this screen with an explanation of these choices, other than a hyperlink to the general (consumer-oriented) Microsoft privacy statement.[45]

Illustration 3: Privacy Options in Office 365 CTR for users[46]

[45] Microsoft does provide some information about this choice in the Home version of Office, namely: *When you select Let Office connect to online services from Microsoft to provide functionality that's relevant to your usage and preferences, Office connects to online services and sites provided by Microsoft, such as Bing Maps, Insights, and Bing Weather."*

[46] Screenshot from public Microsoft documentation, URL: https://support.office.com/en-us/article/view-my-options-and-settings-in-the-microsoft-office-trust-center-d672876e-20d3-4ad3-a178-343d044e05c8 .



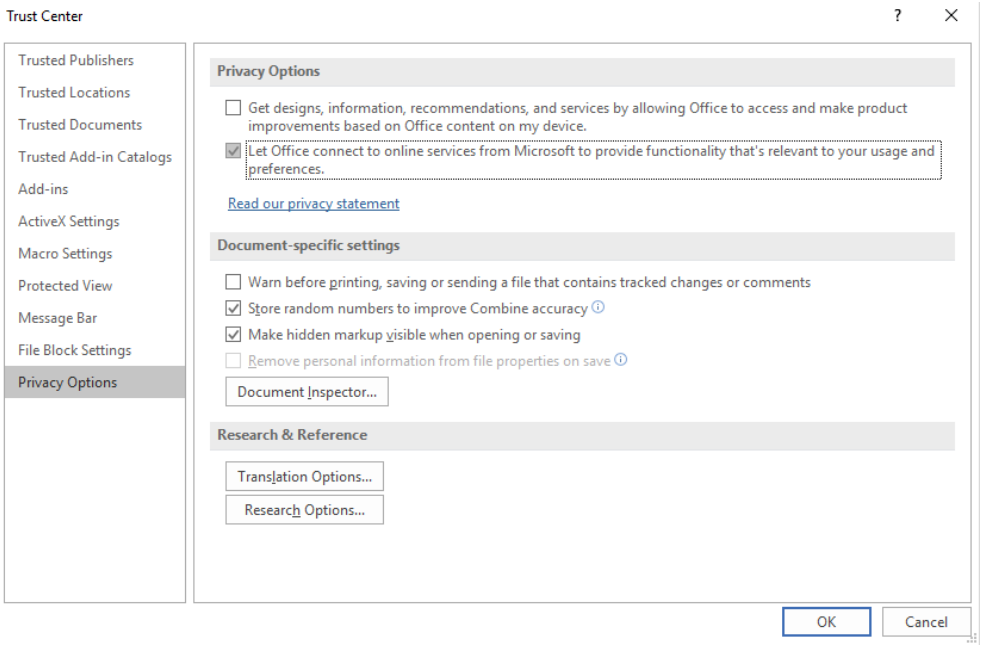
Individual users are able to change the privacy settings for the first option (to make improvements to Office). Microsoft allows all users to individually tick the check box in the Trust Center accessible through all programs, to send personal information to Microsoft to make improvements to Office. However, admins can prevent users from selecting this option by using the Office Customization Tool or by setting Group Policy Objects. [47]

There is no direct information on screen what kind of personal data Microsoft collects if a user ticks the box to *Send personal information to make improvements to Office*.[48]

[47] For a manual, see: https://config.office.com/. The idea of a Group Policy setting is that a user is made to get a pop-up with a warning that the admin prohibits a certain option or choice. A Group Policy setting will override any user choices after some time, by default after 90 minutes.

[48] Microsoft claims in its written response of 24 September 2018 that there would be information if a user clicked on the question mark in the top right corner. This is not the case. In the Office 2016 MST install used for this DPIA, the question mark leads to a generic explanation about Word add-ins and code samples. The URL is: https://docs.microsoft.com/en-us/office/client-developer/word/word-home. In the Office 365 install, the text leads to a generic help page with 'Top help topics' that does not contain any information to answer this question. The URL is: https://support.office.com/en-us/article/top-help-topics-641ee4c4-a616-45dd-b7da-4cb03c12ad6e?lcid=1033&NS=WINWORD&Version=16&ShowNav=False&syslcid=1033&uilcid=1033&ui=en-US&rs=en-US&ad=US

Illustration 4: Privacy Options in Office 2016 MST for users[49]



If a user would search the Microsoft support pages about the Trust Center, she could find some public information about this choice at the bottom of a support page. The explanation Microsoft provides, is:

> *"Microsoft automatically collects information from your computer, including the error messages that are generated by the software and when they are generated, the kind of computer equipment that you are using, whether your computer is having any difficulty running Microsoft software, and whether your hardware and software respond well and perform rapidly. In general, this information is collected once each day.*
>
> ***Any information that you share with Microsoft is completely anonymous, and absolutely no information is personally identifiable as being yours.*** *This information is not used in advertising or sales in any way. Microsoft does not share this information with any other company. When you join the program, an identification number is generated randomly. That number is the only identification that is used when you share information with Microsoft. Because the number is completely random, Microsoft cannot trace your information back to you — and neither can anyone else* [accent added by Privacy Company]."[50]

It is not clear why the selection box mentions that a user will send 'personal information', while the explanation is about 'completely anonymous' information that the user shares with Microsoft.

[49] Screenshot from public Microsoft documentation, URL: https://support.office.com/en-us/article/view-my-options-and-settings-in-the-microsoft-office-trust-center-d672876e-20d3-4ad3-a178-343d044e05c8 .
[50] https://support.office.com/en-us/article/view-my-options-and-settings-in-the-microsoft-office-trust-center-d672876e-20d3-4ad3-a178-343d044e05c8

Microsoft has explained that the default setting in the second option (use of the Connected services) is a deliberate choice. However, Microsoft also acknowledges that many customers want to select the setting themselves and receives consistent feedback that all privacy impacting features have to be configured to be Off, unless the tenant switches them On.[51]

The admin of each tenant can only switch off the use of some of these Connected Services, by using the Office Customization Tool or by setting Group Policy. Microsoft explains: *"If an organizational customer does not wish to enable its users to use the small number of ProPlus connected online services for which Microsoft is a data controller (e.g., intelligent services powered by Bing such as translation) these services can be "toggled off" for the entire organization by the IT administrator."*[52] There are 3 choices for the admin, namely:

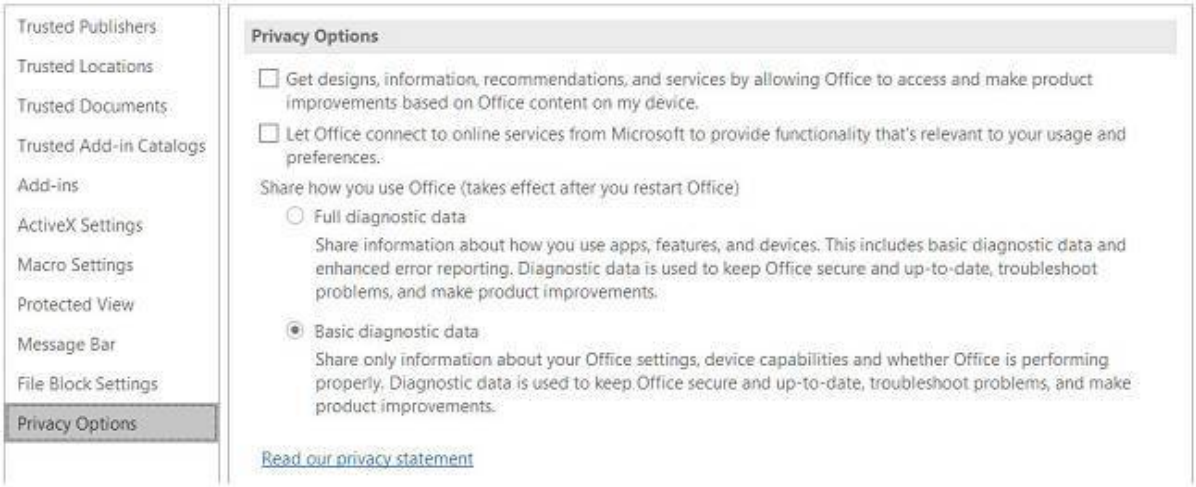
- On for all
- Off for all
- Configurable by the user[53]

It is not possible to centrally switch off the mandatory Connected Services. See Annex 1.

The lab report also shows that if a user uses a Connected Service once, in one application, that the default setting for Connected Service in all applications in Office is changed. This has been observed in devices running Windows, MacOS and iOS. According to Microsoft this is intentional design. Within Office, the four main applications share tools, and therefore, the consent is configured for Connected services in all Office products.[54] For a short period, Office offered a third option, to select between Basic and Full Office telemetry data.[55] This option was added to the privacy choices in May 2018, but quickly removed.

Illustration 5: Prior additional option in Office to select Full or Basic telemetry[56]

[51] Meeting report 29 August 2018, answer to Q26.
[52] Microsoft Annex 1: Deploying GDPR Compliant Windows 10 Enterprise and Office 365. See also Meeting report 29 August 2018 answer to Q16.
[53] Meeting report 3 September 2018, answer to Q3.
[54] Meeting report 3 September 2018, answer to Q4.
[55] See for example The Register, Microsoft gives users options for Office data slurpage – Basic or Full, 24 May 2018, URL: https://www.theregister.co.uk/2018/05/24/microsoft_word_2016_data_diagnostics/
[56] Screenshot from MacOS in The Register, https://www.theregister.co.uk/2018/05/24/microsoft_word_2016_data_diagnostics/ .



Microsoft has explained that the roll-out of these options was removed quickly. The settings never made a difference.[57]

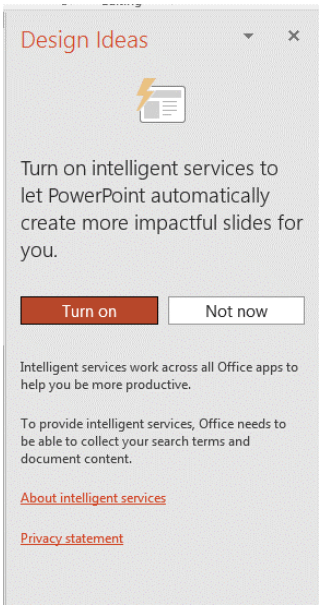


Illustration 6: pop-up in PowerPoint with recommendation to turn on intelligent services

There is a fourth option for users to influence the processing of Office diagnostic data by Microsoft. This option is only available when Microsoft shows a recommendation on screen to use another product or service from Microsoft.

It is currently not possible for either users or tenants to switch off the processing of diagnostic data for this purpose of showing targeted recommendations. Microsoft has stated: *It is not possible to switch this service off. Users don't want a service where the users don't know how to use it.*[58]

Microsoft has explained that it consciously only provides the options 'Turn on' and 'Not now' to users. There is no option for users to switch these recommendations off completely, for example with a 'Never' button. Microsoft has explained that it is aware of complaints about these pop-ups[59], but it is a minority of users. "*If we were to shut if off completely, our customers, especially students and younger people would look for a different product online. This choice is incentivised by commercial realities. With the recommendations we*

[57] Meeting report 29 August 2018, Answer to Q27. The choice still does exist in Office for the MacOS. Microsoft has explained that client bits are hard to change, and that that is even harder on MacOS (for Microsoft).
[58] Meeting report 29 August 2018, answer to Q16.
[59] See for example, https://answers.microsoft.com/en-us/msoffice/forum/msoffice_other-mso_mac-mso_mac2016/share-how-you-use-office-popup-how-can-i-turn-this/1ecaf16f-7247-47bb-bd93-13193f4377ce

protect the monetisation of the Office product, and we accept we have to disrupt the attention of the users."[60]

4. Purposes of the processing

Because Microsoft does not treat diagnostic data as a separate category of data, the contractual framework between Microsoft and SLM Rijk does not mention or define (the privacy protection of), diagnostic data. This framework relies on amendments on the Online Service Terms (OST). The OST generally describe Microsoft's activities as a data processor. However, with regard to some additional, discretionary Connected Services, Microsoft considers itself to be a data controller. Following the Dutch government PIA model, these roles will be described in more detail in section 5 of this report, including the differences between Microsoft Ireland as the office signing the contract, and Microsoft Corporation as a data controller in the general Privacy Statement.

Microsoft does not provide a clear overview of the purposes for which the diagnostic data are processed. For instance, the OST mention: *Microsoft may recommend or download to Customer's devices updates or supplements to this software, with or without notice.* (…) *The Apps may collect data about the use and performance of the Apps, which may be transmitted to Microsoft and used for the purposes described in this OST for Customer Data.*[61] According to Microsoft, these particular sentences allow Microsoft to use the collected diagnostic data to show recommendations.[62]

Microsoft acknowledges that there is no specific documentation about the use of diagnostic data from the mandatory Connected Services.[63]The Dutch government amendment on the Business and Services Agreement, Customer Data are explicitly defined to include data *generated* by the use of Online Services. In practice though, this only protects content data actively provided by users when they use the mandatory Connected Services, but not the behavioural metadata that Microsoft collects and stores as a result of the use of the Online Services. The amendment also specifies that Microsoft may not use Customer Data for compatible purposes.[64] Again, this does not apply to the behavioural metadata collected in system-generated event logs and telemetry data.

In the OST, Microsoft specifies that it "*will not use or otherwise process Customer Data or derive information from it for any advertising or similar commercial purposes*." Again, this does not provide any guarantees with regard to the purposes of the processing of the behavioural metadata and telemetry data. And according to Microsoft, the serving of targeted recommendations as shown in illustration 6, would *not* be an advertising or similar commercial purpose.

[60] Meeting report 3 September 2018, answer to Q5.
[61] OST September 2018, p. 5
[62] Meeting report 3 September 2018, new question.
[63] Meeting report 28 August 2018, answer to Q6. *For each of the connected services, there is a document in which the functioning is described. This does not include specific purposes for telemetry.*
[64] Microsoft Business and Services Agreement, Amendement ID CTM, May 2017, p. 10, replacement of the paragraph General conditions for privacy and security in the OST.

According to Microsoft, the Office diagnostic data are necessary to provide the service, and this includes four sub purposes.

The diagnostic data are used to ensure the service is always:

1. secure,
2. functioning,
3. up to date, and
4. evolving.

According to Microsoft, the showing of pop-ups with recommendations to use certain features or use other Microsoft products, is part of this purpose, or at least, compatible with this purpose. Microsoft has explained:

> *We will recommend to users services that are included in their contract, such as a tip when you are working in Word, that you can better protect your document, if you have contracted both Office and the Protecting service. We don't call it a recommendation, we call it advice on efficient usage. If you start up Word, a recommendation may be given to use a specific feature. Or in Excel, a suggestion to create graphs. This unsolicited advice is not marketing or advertising, because we are not selling anything, the customer already has bought all the functionality. We are just telling the user how to better use our products.*[65]

In the dialogue with Microsoft representatives, Microsoft has mentioned another additional purpose for the processing of Office diagnostic data, the creation of inferred data based on audit logs and Customer Data.

> *"For example to learn about the workload in a given enterprise and prevent storage of multiple copies. This type of processing falls under the general sub purpose of making the service cheaper, thus improving the service. MS does not consider it necessary to detail the sub purposes. This is part of the reason to contract the services, that MS will deliver them robustly and securely."*[66]

It is not clear how Microsoft delineates the purpose of ensuring that the service is always evolving. Microsoft has mentioned a general need to use data to improve services and develop new products: "*We need data to create new products, to improve services and for new product development. We use machine learning analysis to detect what is happening. Businesses for example want a better search engine to find documents/content and people."*[67]

In response to this DPIA, Microsoft has stated that there are 3 purposes for the processing of the diagnostic data (as defined in this report), namely:

- Secure means security threats and risks are identified and mitigated as quickly as possible
  through updates to Office ProPlus Applications and remediation of connected services.

[65] Meeting report 29 August 2018, answer to Q16.
[66] Meeting report 29 August 2018, answer to Q17.
[67] Meeting report 30 August 2018, answer to Q46.

- Up to Date means all the latest updates to the Office ProPlus Applications are delivered and installed without disruption to the experience.
- Performing Properly means anomalies, "bugs," and other product issues are identified and mitigated as quickly as possible through updates to the Office ProPlus Applications and remediation of connected services.[68]

Microsoft has **not denied** in either of its responses to this section of the DPIA that the purposes mentioned above are included in these 3 purposes. Microsoft has explicitly stated that it does not think it is necessary to explain any sub-purposes. 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.[69] Therefore, this report assumes that Microsoft processes the diagnostic data for the following 8 purposes.

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)
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 7 purposes.

In its response of 1 October to this DPIA report, Microsoft explains that the company processes the personal data contained in the system-generated event logs for the same purposes as the Customer data, and this includes all compatible purposes.[70]

The only explicit denial from Microsoft concerns further processing of content data collected through mandatory Connected Services. Microsoft will not use those data for compatible purposes.[71]

These 8 purposes only apply to the diagnostic data from services for which Microsoft considers itself to be a data processor.

[68] Microsoft confidential response to this DPIA report, 24 September 2018, p. 5.
[69] Microsoft confidential answer 1 October 2018 to the 10 follow-up questions, answer Q5b.
[70] 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*.
[71] Idem, p.

With regard to the diagnostic data about the use of the (additional) discretionary Connected Services, Microsoft Microsoft considers itself to be a data controller, and processes diagnostic data about the use of the voluntary Connected services for all of the purposes mentioned in its general Privacy Statement.[72]

Before describing the (long list of) purposes for which Microsoft may process personal data according to its general Privacy Statement when it considers itself to be a data controller, this report first outlines the issue of compliance with law enforcement orders, since this is also relevant for Microsoft as a data processor.

Disclosure to law enforcement

As a data controller, Microsoft may be obliged to hand over personal data to law enforcement. Microsoft publishes a bi-annual transparency report. In the Netherlands, in the period July-December 207, Microsoft received 310 requests, relating to 374 accounts/users.[73] Microsoft also explains that very few of law enforcement requests relate to Enterprise cloud customers.[74] 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 *tenant* cannot be trusted.

In its general privacy statement, Microsoft mentions the purpose of legal compliance, with the following explanation: "*We process data to comply with law. For example, we use customers' age to ensure we meet our obligations to protect children's privacy. We also process contact information and credentials to help customers exercise their data protection rights.*"[75]

Microsoft also 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.*"[76] 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.[77]

---

[72] Microsoft Privacy Statement, with monthly changes, version used for this DPIA was last Updated: August 2018, available at https://privacy.microsoft.com/en-GB/privacystatement .In its confidential answer of 1 October 2018, answer 4C, Microsoft confirms that it processes the diagnostic data from the voluntary Connected Services for all purposes in the general privacy policy.

[73] Microsoft Law Enforcement Requests Report, URL: https://www.microsoft.com/en-us/about/corporate-responsibility/lerr

[74] Idem. *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 noncontent information only. Three of the requests are still pending resolution*.

[75] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement.

[76] OST September 2018, p. 7.

[77] OST September 2018, p. 7.

This provision in the OST is drafted in such a way as to only apply to Customer Data, while it is outlined in the section 3 in this report that Microsoft does not consider telemetry data to be part of the Customer Data. With regard to other diagnostic data (the system-generated event logs and content actively provided by the user when using a Connected Service) Microsoft follows an opaque approach, as Microsoft may consider these data to be either anonymous, or personal data or Customer Data. All of these diagnostic data may be valuable to law enforcement and therefore subject to a disclosure order.

Purposes outlined in the General Privacy Statement

When Microsoft considers itself to be a data controller, such as when processing diagnostic data from discretionary Connected services, all the purposes mentioned in Microsoft's general Privacy Statement apply.[78]

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.[79]

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."*[80]

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. We also communicate*

[78] 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*.

[79] These are the following purposes: Customer support, Promotional communications, Relevant offers, Advertising, Transacting commerce.

[80] Microsoft Privacy Statement, Product-specific details: Enterprise and developer products, available at https://privacy.microsoft.com/en-GB/privacystatement.

with you to secure our products, for example by letting you know when product updates are available."[81]

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.*"[82]

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.*"[83]

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.*"[84]

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.*"[85]

7. Purpose: Help secure and troubleshoot

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

---

[81] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement.
[82] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement
[83] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement
[84] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement
[85] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement

"*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.*"[86]

8. Purpose: Safety

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

"*We use data to protect the safety of our products and our customers. Our security features and products can disrupt the operation of malicious software and notify users if malicious software is found on their devices. For example, some of our products, such as Outlook or OneDrive, systematically scan content in an automated manner to identify suspected spam, viruses, abusive actions or URLs that have been flagged as fraud, phishing or malware links; and we reserve the right to block delivery of a communication or remove content if it violates our terms.*"[87]

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.*"[88]

10. 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.*"[89]

11. 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.*"[90]

---

[86] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement
[87] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement
[88] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement
[89] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement
[90] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement

12. *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.*"[91]

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 8 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 3 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

As will be explained below, the first scenario is desirable with regard to all Office diagnostic data, but based on a factual and formal analysis, Microsoft does not behave like a data processor with regard to any of the diagnostic data. The third scenario (Microsoft as a unique data controller) can only theoretically apply to the collection of diagnostic data about the use of some Connected Services. As will be explained below, Microsoft and the Office Enterprise customers have to be qualified as joint controllers for all diagnostic data collected through any connected service.

Even though the Dutch government organisations sign a contract with Microsoft Ireland, the data controller for 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

[91] Microsoft Privacy Statement, under "How We Use Personal Data", available at https://privacy.microsoft.com/en-GB/privacystatement

signed by, Microsoft Corporation. The USA mother organisation is also the data controller with regard to the voluntary Connected Services, since Corporation determines the global purposes and means for the processing.[92] Additionally, MS has already confirmed that all Office telemetry data are sent to a single end-point in the USA, where engineers from Microsoft Corporation may use the diagnostic data for analysis purposes.

In the first scenario, a governmental organisation deploys Microsoft Office software to carry out some regular work tasks. Following the definition of a data processor, Microsoft may only process the personal data necessary in connection to the exercise of the tasks that are defined by the governmental organisation. In that case, Microsoft could be qualified as a processor for the organisation in question.

But in fact, Microsoft does not conclude classical processing agreements with its Enterprise customers. Instead, the standard terms and conditions of Microsoft apply. As an annex to the OST, the pre-filled EU Standard Contractual Clauses are included.[93] Microsoft's conditions in this context are somewhat rigid. For instance, if Microsoft would only process data as a data processor, it would need to follow the written instructions of the controller. But in its terms, 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.*"[94]

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.[95] SLM Rijk has managed, as the federal supply management office, 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 repeats that the contract and use of features provide a complete list of instructions:

> "*The Enrolment (including these GDPR terms), along with Customer's use and configuration of features in the Online Services, are Customer's complete and final instructions to Microsoft for the processing of personal data.*"[96]

Microsoft claims that this practice is approved by the data protection authorities in the EU.[97] Microsoft includes a list of 108 sub-processors in its terms and conditions, and claims that no

[92] The Dutch DPA provides a detailed explanation of the roles of Microsoft Corporation, Microsoft Ireland and Microsoft Netherlands B.V. in its Windows 10 telemetry investigation report. See paragraph 2.2 of this report. In sum, Microsoft Ireland is a relevant establishment of Microsoft Corporation, but the role of establishment should not be confused with the role of data controller. See pages 105-112 of the Dutch DPA report.
[93] Microsoft European Union model clauses backgrounder, URL: https://aka.ms/eu-model-backgrounder (January 2017).
[94] OST September 2018, 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'.
[95] OST September 2018, p. 8.
[96] Additional GDPR Terms included in Annex 1 to the GDPR Terms, Amendment ID M434, April 2017.
[97] Microsoft confidential response to this DPIA report, 24 September 2018, p. 18.

single data protection authority has objected against this.[98] This means that the government institutions have to give blanket consent to all sub-processors used by Microsoft. It is unlikely that Microsoft would be willing to stop its cooperation with any sub-processor if SLM Rijk, or any of the tenants, would object.

Another important element of the EU Standard Contractual Clauses is the ability for the data controller to audit the data processing by the data processor.[99] This enables the data controller (the Enterprise customer) to guarantee that the data processing is in accordance with the high level of data protection granted in the EU. SLM Rijk has not been able to negotiate the ability to add audit questions to the audit frame, in particular with regard to sub-processors. In an amendment on the Online Service Terms, Microsoft hesitantly agrees to take a suggestion for other audit questions in consideration, but Microsoft has also indicated during the meetings with SLM Rijk and Privacy Company that Microsoft is not willing to give the Dutch government the same rights to add audit questions as for example the financial services industry in the Netherlands. In view of the fact that some sub-processors are content delivery networks that probably make real-time copies of all data, there is a reasonable likelihood that these sub-processors can process the diagnostic data for unauthorised purposes. Microsoft says that the right to audit is not removed from its pre-filled EU Standard Contractual Clauses, but there is a high price attached to such a request. [100]

Specifically with regard to concerns about access to Customer Data, including personal data, and further processing by sub-processors, Microsoft has given the reassurance that Microsoft itself governs the access from all sub-processors to Customer Data, including personal data.

> "*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.*

[98] Meeting report 30 August 2018, answer to Q43. In its Compliance Manager Office 365, tab 'Microsoft Managed' Microsoft explains: *Customers may download a current list of [Office 365 Subcontractors](http://go.microsoft.com/fwlink/?LinkId=213175&clcid=0x409) from Microsoft's Web site. Customers who subscribe to compliance notifications are notified when a new subcontractor is added to Office 365. Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the Data Processing Terms of the [Microsoft Online Services Terms] (http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31).*

[99] 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 this 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.

[100] Meeting report 30 August 2018, answer to Q44. Confirmed by Microsoft in its confidential response to this DPIA report, 24 September 2018, p. 22-23.

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."[101]

While Microsoft has attached quite some safeguards to the access of sub-processors to the classes of data Microsoft deems confidential, such as Customer Data and personal data, no guarantees are provided with regard to diagnostic data. Additionally, the audits organised by Microsoft examine the structure of rules and the existence of checks, but not how the data are factually processed.

During the meetings with SLM Rijk and Privacy Company, Microsoft acknowledged there's a heightened risk with some sub-processors. Microsoft has agreed to verify the contracts and retention periods with a specific CDN.

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. But 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.[102]

Microsoft does not give copies of its contracts with sub-processors, but is willing, on request, to provide a copy of addenda on the standard contractual clauses.[103]

Assessment Microsoft as a data processor

In view of the fact that there is no comprehensive documentation what kind of personal data Microsoft processes about the individual usage of the Office software, and no clearly defined purposes, in practice the *tenants* cannot fulfil their role as data controllers for the diagnostic data. The alleged 'data controllers' have no clue what personal data the alleged 'data processor' processes on their behalf. It follows from section 4 in this report that Microsoft has determined 7 purposes of the processing. Additionally, Microsoft allows itself to determine what other purposes may be compatible for the processing of diagnostic data (an eight purpose).

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*). But Microsoft has contractually maximised this liberty, and provides no well-defined, clearly delineated purposes that would allow the tenant to be in control.

One of the purposes that Microsoft has described as being compatible, is to show targeted recommendations about its own products. This purpose of this data processing primarily serves Microsoft's economic interest to be able to compete with 'free' competitors. Microsoft does not enable its Enterprise customers to explicitly request Microsoft to perform this data processing. The opposite: Microsoft does not even allow its customers to reject this purpose of the processing. There is no control available for admins to prevent the processing of personal data

[101] Meeting report 30 August 2018, answer to Q40.
[102] Meeting report 30 August 2018, answer to Q40 and Q41.
[103] Meeting report 30 August 2018, answer to Q41.

for this purpose. Additionally, it follows from the above that Microsoft itself determines the scope of the audits.

Microsoft may also take the decision, when ordered to do so, to hand over data to law enforcement. But according to the GDPR, only data controllers may take decisions to hand over personal data to law enforcement.[104]Article 48 of the GDPR creates an exception to this rule, acknowledging that a data processor may sometimes be forced by a court or administrative authority in a third country, outside of the EU, to transfer or disclose personal data. That may only be recognised or enforceable if it is based on an international agreement such as a mutual legal assistance treaty. This exception is titled 'Transfers or disclosures not authorised by Union law'. This exception therefore does not change the main rule that only data controllers may take decisions to hand over personal data.[105]

Finally, as will be described in section 10 of this DPIA, Microsoft determines the retention period for 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.*"[106]

Determining how long data can be stored, is also 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.

In sum, based on a factual analysis who determines the types of personal data that are processed for what purposes, including hand-over to law enforcement and processing for compatible purposes, and who decides about the scope of the audits and the retention period, Microsoft cannot be qualified as a data processor for the processing of Office diagnostic data. By taking these decisions, Microsoft acts a a data controller. However, Microsoft is not the only data controller responsible for the processing of personal data via diagnostic data. In the current circumstances, it is more likely that the second scenario applies, of joint controllership.

Assessment Microsoft and tenants as joint controllers for most diagnostic data

The European Court of Justice has clarified in two recent rulings[107] 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

[104] See for example the controller-processor opinion WP 169 from the Article 29 Working Party, p. 11, about the SWIFT-case: "*The fact itself that somebody determines how personal data are processed may entail the qualification of data controller, even though this qualification arises outside the scope of a contractual relation or is explicitly excluded by a contract. A clear example of this was the SWIFT case, whereby this company took the decision to make available certain personal data - which were originally processed for commercial purposes on behalf of financial institutions - also for the purpose of the fight against terrorism financing, as requested by subpoenas issued by the U.S. Treasury*."

[105] Microsoft objects in its response to this DPIA that it is not free to take a decision when it is required to hand-over personal data, but this objection seems to be based on moral principles, not on the legal analysis of the tasks of a data controller and article 48 of the GDPR.

[106] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q8 (preamble).

[107] 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

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.

Office Enterprise Customers have some say about the processing of diagnostic data. As explained in section 3.1 of this report, admins may switch off the processing of some diagnostic data, by not allowing the use of (voluntary) Connected Services, or by not enabling audit logs for security purposes. Even though this influence is limited, and Enterprise customers have very little information or say about the processing of diagnostic data, organisations that choose to use the Office software allow and enable Microsoft to collect and store personal diagnostic data.

To paraphrase the European Court of Justice: the production of statistics (and use of the data to show recommendations to users) about user behaviour in Office is based on the prior collection of event data from the computers or other devices of users of the Office software, and the processing of the personal data of those users for such statistical purposes.[108]

Microsoft has confirmed it is considering the scenario for joint responsibility for the processing of telemetry data from Windows 10 Enterprise. Microsoft underlines that the facts have to be the same to reach the same conclusion for Office, but in principle, Microsoft considers itself to be a data processor for all personal data collected through the use of the mandatory Online Services.[109]

Assessment Microsoft as data controller for the voluntary Connected Services

With regard to the third scenario, Microsoft considers itself to be an (independent) data controller for the diagnostic data it collects via the use of some of the (additional) Connected services. In practice, this situation is very unclear for the end-users of the service. SLM Rijk has tried to bring the discretionary Connected services such as the online spelling checker and the dictionary under the processor agreement. This would allow usage of these functionalities without separate consent of the employees. SLM Rijk wants the processing to take place within the clear processor boundaries, similar to the mandatory Connected Services. Microsoft, however, is not willing to bring the usage data of these discretionary Connected Services in the scope of the Enterprise processor agreement. Microsoft has confirmed that the Dutch government is not the only procurement party interested in bringing the Connected services in line with the Enterprise agreement, but the company has not made any commitment.[110]

According to Microsoft, the Connected Services are 'free' and thus, they are separate from the Office software procured by government. Microsoft states it is up to the *tenants* to establish and

---

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.

[108] European Court of Justice, C-210/16, paragraph 38: *While the audience statistics compiled by Facebook are indeed transmitted to the fan page administrator only in anonymised form, it remains the case that the production of those statistics is based on the prior collection, by means of cookies installed by Facebook on the computers or other devices of visitors to that page, and the processing of the personal data of those visitors for such statistical purposes. In any event, Directive 95/46 does not, where several operators are jointly responsible for the same processing, require each of them to have access to the personal data concerned.*

[109] Microsoft confidential response to this DPIA report, 24 September 2018, p. 16.

[110] Meeting report 29 August 2018, answer to Q16.

enforce a policy and governance for access to any online service, be it a Microsoft controller service such as online spelling checker or the use of another cloud service or online translate service.[111]

This argument does not change the legal assessment that government bears a serious responsibility for the processing of data through the use of these services by its employees. The Connected Services are closely integrated with the use of the Office software. Microsoft also uses the diagnostic content data to present specific recommendations to users to use (other) Connected Services. Because the Connected Services are such an essential part of effective use of Office software, it cannot be expected that employees will say 'No' to a consent request from Microsoft. They have to deliver flawless work, without spelling mistakes, in order to please their employer. Thus, by allowing Microsoft to present an offer they can't refuse to employees, the government institutions are jointly responsible, together with Microsoft, for the processing of personal data about the use of the Connected Services. The only way the *tenants* can prevent this joint controllership, is by switching off the Connected Services completely, at the cost of loosing essential functionality.
The different legal grounds in relation to the roles of processor and (joint) controller will be analysed in section 11 of this report.

6. Interests in the data processing

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

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.

> *"No single customer has the scale or capacity. Customers are looking for cheaper solutions. We are cloud first in development. Cloud deployment at scale, some objectives can only be achieved in the cloud. For example with the on-prem version of SharePoint, you cannot achieve every goal. Associated with scale and intelligence we can provide functional benefits. We obtain security intelligence across threats and industries."*[112]

The interests of Microsoft and the Dutch government align when it comes to the use of diagnostic data to keep the services secure. For the Dutch government, the ability to access data about user behaviour through audit logs is essential to comply with its own obligations as a data controller to detect possible security incidents. However, it is not clear to what extent Microsoft allows itself to use diagnostic data that are processed in the audit logs for other purposes, since the audit data are not covered by the data processor agreement.

[111] Microsoft slides presented on 1 November 2018.
[112] Meeting report 30 August 2018, answer to Q46.

As part of the shared interest in security, Microsoft needs to be able to deliver timely updates of the software.[113] Similarly, the interests are aligned that Microsoft needs to deliver a well-functioning product, for the Dutch government to prevent loss of labour capacity. The Dutch government also has a strong general interest in providing reliable, always on, well integrated, administration tools to its employees. Well-functioning for the Dutch government also means that the software has to be accessible on different devices, and from different locations. The ability for employees to seamlessly work at home allows the Government to cut back spending on work spaces in offices.

However, with regard to other purposes for which Microsoft may process the Office diagnostic data, the interests may not align. This may be the case when Microsoft uses the diagnostic data to develop new services, uses the data to detect usage of products of competitors, or uses the data for inferred learning.

Microsoft 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."*[114]

Microsoft has also spoken about its economic (competition) interest and financial (monetisation) interest in the use of diagnostic data to show advice to the users of the software. Microsoft has explained that this type of advice is 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 scenario's.*[115]

Microsoft has explained why users are not given a choice to switch off recommendations completely. Microsoft has an economic interest in certain default settings. Microsoft has claimed

[113] 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.
[114] Meeting report 30 August 2018, answer to Q46.
[115] Meeting report 29 August 2018, answer to Q16.

that it would suffer economic harm if the default setting for the use of Connected Services was default switched to 'Off'.[116]

Generally speaking, Microsoft has an economic interest in the sales of subscriptions to online services, instead of shipping products. 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. However, 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 Defense has a military state sovereignty interest to only store data in a sovereign cloud.

Microsoft does not offer a sovereign country cloud to countries, with the exception of the cloud for China and cloud for the federal USA government. The costs to build a separate cloud for the Netherlands would be prohibitive, said Microsoft, approximately 90 million US dollar. Microsoft has built its cloud to be able to process data anywhere where it operates (with the exception of China). 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.[117] If Microsoft would have to commit to more local or EU storage, that would involve high costs and be a barrier to innovation, according to Microsoft.[118]

In sum, Microsoft has financial, economic and commercial/business interests in the collection of diagnostic data, and the ability to use it for all the different purposes mentioned above, both as a data controller and as a data processor. Some of these interests align with the Dutch government, but some don't.

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. A special arrangement exists between the United States and the European Union, according to which undertakings may self-certify as to their standard of protection of personal data. Personal data may also be transferred from the EU to a third country using Standard Contractual Clauses, as drafted by the European Commission under the Data Protection Directive. These clauses ensured a high level of protection contractually. Microsoft uses a combination of two measures: Privacy Shield and Model Clauses.

In the Online Service Terms, 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*

[116] Meeting report 29 August 2018, answer to. Q30.
[117] Meeting report 29 August 2018, answer to Q21.
[118] Meeting report 29 August 2018, answer to Q21.

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."[119]

Microsoft has explained that this EU storage commitment only applies to the above mentioned stored Customer Data. It only covers data from what Microsoft defines as 'Core Services'. There is no commitment with regard to the storage in the EU of data about Office 365 ProPlus (as this belongs to the category of 'Other' services).

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 section 10 *Retention Periods*.

The actual storage in different data centers varies per service. This is for example different for Outlook and for SharePoint Customer Data. Access to the Customer Data that Microsoft defines as Core Services is audited following the strict controls of SOC-2. Access to the Customer Data provided by Office 365 ProPlus is audited following the ISO 27001 norms.

As described in section 3 of this report, Microsoft has no documentation which diagnostic data it considers to be Customer Data. Other personal data can be stored anywhere in the world, including diagnostic data.

The specific telemetry data generated by Office are probably only stored in the USA, but this has to be verified. The current endpoint for data collected via the telemetry client is in the USA. 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 the different engineering teams may cut their own cubes (select multidimensional datasets) to analyse.[120]

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. But next to Windows 10 related telemetry data, 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, the technical lab of the ministry of Justice & Security was unable technically (due to the encoding of the data) to inspect the contents of the outgoing data stream. As an essential security measure, and in order to limit the use of the capacity of the end-user device, Microsoft encodes the events, and packages them in the outgoing traffic to its own servers. Microsoft did not (yet) provide tools to the lab to decode the outgoing data stream or view the contents of the traffic in another way.

[119] OST September 2018, p. 10.
[120] Meeting report 29 August 2018, answer to Q21.

Therefore the description of the techniques and methods of the data processing remains general, and is mostly based on statements made by the Microsoft delegation.

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. 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.[121]

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.[122] Through this telemetry client, Microsoft also collects diagnostic data about the use of additional (processor based) Connected services offered by Microsoft in combination with the key Office applications.

Besides the processing via the telemetry client, Microsoft collects diagnostic data via system-generated event logs, such as the security audit logs, but also through system generated logs about the use of controller based Connected Services as for example an online spelling checker or dictionary.

If Microsoft would store data that it collects for functional use, such as snapshots of the software to provide updates, or data exchanged to allow users to authenticate, they would also become diagnostic data that can be used to analyse individual usage of the Office software.

Big data processing

There is no comprehensive documentation about the content of the diagnostic events collected by the use of the Office software. Microsoft has confirmed: "*There's no documentation or overview or summary of the telemetry collected by the Office software. That's true for event data in the Office client. But also true for the event data in intelligent services that you're using.*"[123] Microsoft has also explained that until recently, there were no central rules governing the collection of telemetry data.[124] Currently, 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.*" [125]

[121] Microsoft confidential response to this DPIA report, 24 September 2018, p. 6.
[122] Meeting report 28 August, answer to Q7.
[123] Meeting report 28 August 2018, answer to Q6.
[124] Meeting report 28 August 2018, answer to Q1.
[125] Microsoft confidential response to this DPIA report, 24 September 2018, p. 10.

With Office telemetry Microsoft collects 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.*[126]

Microsoft has explained that there are 150 custom fields which may be used to collect the diagnostic data. "*The 150 custom fields have no predefined content, are changed dynamically and the collected telemetry data will change frequently.*[127]

Microsoft has committed to develop documentation.

Solely automated decisions

Microsoft has stated it may collect a specific event from all users (sample rate 100%), but collects most of the telemetry events from only 2% of the user population.

Microsoft has confirmed that Office does not show users if they have been selected for the (limited or full) sample of telemetry, and Microsoft does not plan to develop such a functionality.[128] In fact, the selection of a user for the collection of (additional) telemetry data is a decision based solely on automated processing. And because the process is not transparent, Microsoft does not allow employees the right to obtain human intervention to contest this decision, either with their employer (*the tenant*) or with Microsoft. Though this solely automated decision does not produce a legal or other significant effects as required by article 22 of the GDPR, this lack of transparency poses an extra risk for certain types of employers and employees.

Local versus cloud use of Office software

Enterprise customers can install the Office ProPlus software in four different ways.

1. Office 2016 installed entirely local, without a Microsoft Enterprise account[129];
2. Office 2016 installed on the local device with a possibility to use limited cloud services[130];
3. Office 365 installed locally via the Click To Run method[131];
4. Office 365 web based.

[126] Meeting report 28 August 2018, answer to Q1.
[127] Meeting report 28 August 2018, answer to Q5.
[128] Meeting report 28 August 2018, answer to Q4.
[129] Office 2016 MST installed on the device of the end-user with a local account. The data storage is only local, on-premise. The user connects with a local ID and does not authenticate to an identity server of the Government or Microsoft Azure Cloud. Build 1806 was tested.
[130] Office 2016 Hybrid software installed on the device of the end-user, with a Microsoft Enterprise account. The user connects with a local ID to a government (Office and Windows) authentication server. This local Active Directory server syncs with the Microsoft Azure Cloud. The data storage is local, on-premise. This set-up allows for the possibility to use OneDrive for Business and SharePoint online;
[131] Office 365 Click To Run, with a Microsoft Enterprise account. The set-up is the same as in scenario (ii), but the Office 365 software offers more functionalities compared to Office 2016. Build 1708 was tested.

The Dutch government currently only uses options 2 and 3. In these set-ups, all data storage is on-premise, in the governmental data centres. The Dutch government is testing a hybrid cloud combination, between options 2 and 3. In this new set-up, the content data are still stored in in the local data centres of the Dutch government (on-premise), but in this test, users can use the web-only version of Office 365, and use additional Office 365 cloud services such as the Online Exchange server and Skype. The use of web based Office has briefly been tested as Proof of Concept.

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 Services, (an association with) a Microsoft account is required.[132]

In the first 3 cases, Microsoft collects telemetry data from the in-built telemetry client about the use of the Office software. It is not clear what other diagnostic data Microsoft collects about the use of the Office software via het system-generated event logs, and if there is a difference between these first 3 set-ups. In the fourth case, there is no documentation what kinds of diagnostic data Microsoft collects.

9. Additional legal obligations: ePrivacy Directive

In this section, 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.

It follows from section 2 in this report that Microsoft processes personal data via the diagnostic data about the use of the Office software. Section 5 argues that the Dutch government and Microsoft are generally joint data controllers for this data processing. Based on article 3(1) of the GDPR, because the processing takes place in the context of the activities of the employers based in the Netherlands, the regulation applies to all phases of the processing of these data.

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. Microsoft's denial of the applicability of this provision to the sending of information

[132] In the lab report, in scenario 4.2.2 Test case 2, an Office 2016 MST install switches on 'Connected services', without having to log-in to a Microsoft account. Perhaps in such circumstances a kind of 'shadow account' is created, with a Live ID, in order to allow access to the Connected Services.

through its telemetry client has already been extensively rejected by the Dutch DPA and therefore does not merit any further explanation in this report.[133]

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.

Similarly far reaching, the proposed ePrivacy Regulation contains separate rules about the possibility to automatically distribute updates to users. The proposed ePrivacy Regulation will also broaden its scope to other providers of communication services. Microsoft and the government organisations therefore have to take the principle into account that all traffic data have to be deleted or immediately anonymised after the data have been used to transmit the communication, unless a legal exception applies.

On 10 January 2017, the European Commission published a proposal for a new ePrivacy Regulation.[134] 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.[135] It added a specific exception for updates and with regard to 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*

[133] Dutch DPA, report of findings Microsoft Windows 10, the processing of personal data via telemetry (in Dutch only), Appendix 1, p. 26.
[134] 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
[135] 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

(iii) it is not further used for monitoring the employee.

The Council of ministers has been debating the proposal since October 2017.[136] In the last publicly available version of the proposal, published on 19 October 2018, the ministers propose a similar exception for software updates, not limited to security updates. The ministers also intend to allow employers to seek the consent of employees, without any considerations about the conflict this will cause with the GDPR.

(Art 8 (1) 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; [137]

The Council also proposes to insert a similar exception for security purposes in the use of electronic communications data, in Art. 6:

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.

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*

[136] 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 .

[137]. Council report 19 October 2018, URL: https://www.parlament.gv.at/PAKT/EU/XXVI/EU/03/91/EU_39172/imfname_10848802.pdf. See also: Council report 20 September 2018, ST 12336 2018 INIT, URL: https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=consil:ST_12336_2018_INIT. See also: Council report 10 July 2018, ST 10975 2018 INIT, amendments 19a and 21a.URL: https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=consil:ST_10975_2018_INIT

person, such as an employee, to make use of the service. In such case, consent needs to be obtained from the individual concerned.

10. Retention Period

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.[138]

Outside of the OST or Enrolment documents, Microsoft publishes a separate table with retention periods for active and for passive deletion in Office 365. Passive deletion occurs if a tenant ends the subscription; active deletion when a user deletes data, or an admin deletes a user.[139] As a result of this DPIA, Microsoft has updated the information in this table. Microsoft now states that personal data outside of the Customer Data will be deleted after at most 180 days of the end of the subscription. The updated table no longer provides any explanation about the retention of system-generated event logs or telemetry events. In its response from 1 October to the 10 follow-up questions, Microsoft has confirmed that the personal data in the system-generated event logs will similarly be stored up until half a year after the end of subscription.[140] Initially, during the meetings about this DPIA, Microsoft stated the Office telemetry data were stored indefinitely. In response to this DPIA report, Microsoft has stated it has 2 different retention periods for the Office telemetry data.

After arriving at the Microsoft endpoint, the packets are decoded and broken down into the separate events that were included in the upload. The separate events are then directed into two data stores. The first data store is optimized for quick access and ease of querying. This store only retains the data for 30 days and then it is expunged from the store. The second data store is optimized for longer-term storage and high volumes of data. This store will retain the diagnostic data for no more than 18 months unless a longer retention period is permitted or required by law [see the Data Retention section below].

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.*"[141]

---

[138] OST September 2018, p. 10: "*Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data within an additional 90 days, unless Microsoft is permitted or required by applicable law to retain such data or authorized in this agreement.*"

[139] https://docs.microsoft.com/nl-nl/office365/securitycompliance/office-365-data-retention-deletion-and-destruction-overview (updated 21 September 2018).

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

[141] 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.

In its response to this DPIA, Microsoft ads that this period of 180 days to store diagnostic data may be longer, if a longer period *is necessary to provide and keep Office ProPlus secure, up to date, and performing properly as part of Microsoft's fulfillment of our obligations to all data controller customers to implement and maintain appropriate technical and organizational measures for ensuring the security of processing*.[142] No maximum retention period is mentioned. Additionally, since the different engineering teams may export their own data subsets, and Microsoft does not mention any retention periods for such datasets outside of Cosmos, the actual retention period has to be considered unlimited.

Microsoft explains that the *tenants* cannot change the retention periods of the diagnostic data. Microsoft writes: "*customer-specific diagnostic data retention practices are not supported. The Online Services are a hyperscale public cloud delivered with standardized service capabilities made available to all customers. Beyond configurations available to the customer in the services, there is no possibility to vary operations at a per-customer level. Accordingly, we cannot support a customer-specific commitment related to storage duration for diagnostic data.*"[143]

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.[144]

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.[145] 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.*"[146]

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

[142] Microsoft confidential response to this DPIA report, 24 September 2018, p. 20.
[143] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q8 (preamble).
[144] Idem, answer Q8b.
[145] Meeting report 30 August 2018, answer to Q33.
[146] Microsoft, Data Retention, Deletion, and Destruction in Office 365, URL: https://docs.microsoft.com/nl-nl/office365/securitycompliance/office-365-data-retention-deletion-and-destruction-overview.

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."[147]

[147] 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-5987-45b7-8591-235c4a2f2ca2row 28.

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. In this case, 5 of the 6 legal grounds can theoretically apply to the processing of diagnostic data.

As analysed in section 5 of this report, Microsoft and the Dutch government are joint controllers for the processing of all diagnostic data. Even though Microsoft claims to be a data processor for most diagnostic data, Microsoft performs too many independent tasks, such as the determination of purposes, types of personal data, right to audit and retention periods, to be considered a data processor. This section concludes that Microsoft and the government organisations that use the Office software, are joint controllers for most of the diagnostic data processing.

Microsoft also considers itself to be an independent data controller for the diagnostic data about the use of some voluntary Connected Services. This qualification is not correct either. By allowing Microsoft to present an offer they can't refuse to employees, the government institutions are responsible, together with Microsoft, for the processing of personal data about the use of the Connected Services. The only way the *tenants* can prevent this joint controllership, is by switching off the Connected Services completely, at the cost of loosing essential functionality.

Below, the different possible legal grounds are assessed for the different purposes of the processing. Only the ground of vital interest is not discussed, since nor Microsoft nor the government have a vital (life saving) interest in the processing of the diagnostic data.[148]

Microsoft does not specify the legal grounds for the processing of diagnostic data in any of the different documents in the Enrolment contract. This is logical from the perspective that Microsoft would be a data processor, since data processors may lean on the legal ground from their commissioning data controllers. In its response to this DPIA report, Microsoft claims it can rely on the legal ground for the processing of diagnostic data in the legal obligation for both controllers and processors to comply with the security requirements of the GDPR.[149]

The only exception is the collection of diagnostic data about the use of some of the Connected Services, when Microsoft considers itself to be an independent data controller. In that case, all

[148] Microsoft mistakenly claimed in its initial response to this 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.

[149] Microsoft confidential response to this DPIA report, 24 September 2018, p. 15.

the purposes in the privacy statement apply. In its privacy statement Microsoft states that the different purposes may be based on different legal grounds, but MS 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*".[150]

In its response to this DPIA report, Microsoft claims to rely on three legal grounds for the processing, namely: necessity to perform a contract, necessity for a legitimate interest and necessity for the public interest.[151]

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. MS and government Enterprise customers as a (joint) controllers for the diagnostic data (incl. mandatory Connected services)

This legal ground is not applicable, because nor Microsoft nor the government organisations ask for consent from the employees. For the employers, it is almost impossible to obtain valid, freely given consent from employees, given the clear imbalance in the labour relationship.

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

Additionally, this legal ground is not applicable to the natural persons whose personal data may occur in the diagnostic data. Users of an Office application cannot give consent on behalf of other data subjects (non-users of the service).

Microsoft does not claim to rely on consent for the different privacy options, but offers a possibility for users to select "*Send personal information to Microsoft to make improvements to Office*." If the legal ground is not consent, it is very unclear why users are given an option.

b. MS and government Enterprise customers as (joint) controllers for the diagnostic data about certain discretionary Connected Services.

If the admin of an Enterprise Customer does not centrally prohibit the use of Connected Services, by default the option is switched on: "*Let Office connect to online services from Microsoft to*

[150] Microsoft Privacy Statement, under "Personal Data We Collect", available at https://privacy.microsoft.com/en-GB/privacystatement

[151] Microsoft confidential response to this DPIA report, 24 September 2018, p. 16 and 17.

provide functionality that's relevant to your usage and preferences." See illustrations 3 and 4 in this report, with the different privacy options for end-users.

Microsoft correctly does not consider the legal ground for this processing to be consent. 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*."

Subsidiarily, nor the user nor the government institutions can withdraw consent without detriment. The use of some Connected Services, such as an online dictionary, may be essential for employees to properly perform their work, while they are not free to to install other apps/tools on their devices with similar functionalities.

Additionally, Microsoft does not meet the requirements of specific and informed consent, because of the lack of explanation. Microsoft also cannot obtain consent from users of its product for the processing of personal data relating to non-users.

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. MS and government Enterprise customers as (joint) controllers for the diagnostic data (incl. mandatory Connected services)

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, both that organisation and Microsoft as joint controllers may successfully appeal to this legal ground. This could apply to a limited set of personal data, for a limited set of purposes, such as for example the use of some telemetry data to fix technical errors in the software.

But in the current situation, not all diagnostic data are strictly necessary for the performance of the contract (from government) with the user. If you can perform the service without all of some of the data, (if there is an opt-out), the processing is not necessary. Section 4 of this report describes two existing ways for the admins of Enterprise customers to switch off the processing of some types of diagnostic data (centrally prohibiting the voluntary Connected Services and centrally prohibiting sending data to Microsoft to 'improve' the services). Additionally, Microsoft has made a commitment to help the Dutch government with Group Policy settings to minimise the collection of telemetry data, similar to the Reg Key settings provided for Office 2013.[152].

[152]E-mail Microsoft 25 July 2018 to SLM Rijk, containing the authoritative response for Microsoft Corporation with regard to Reg Key settings provided earlier to block the telemetry flow from Office 2013. In its response from 1 October 2018 to this DPIA report, answer to Q2, Microsoft confirms that it is committed to minimise the flow of diagnostic data from Office 2016/365 using the Reg Key.

With the help of the zero-exhaust settings, and in the future, with in built telemetry level switches, *tenants* may limit the processing of (some) Office diagnostic data. Therefore all current data that are collected on top of this minimum standard, do not comply with the requirement of strict necessity.

For the Dutch government organisations to be able to rely on this legal ground after the application of the zero-exhaust settings, they must check the information they currently provide to staff about the monitoring of employee behaviour, engage in a dialogue with the workers council and update this information where possible.

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

b. MS and government Enterprise customers as (joint) controllers for the diagnostic data about certain discretionary Connected Services.

In its response to this DPIA, Microsoft claims it can rely on the legal ground of contract, since employees would freely sign a separate contract with Microsoft by ticking the box to use Connected Services.[153] This argument is incorrect for multiple reasons.

First of all, employees have a contract with their employer, 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.

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.[154]

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.

[153] Microsoft confidential response to this DPIA report, 24 September 2018, p. 16 and 17.

[154] 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.

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. MS and government Enterprise customers as a (joint) controllers for all diagnostic data (incl. all mandatory Connected services)

This legal ground can only be invoked for one specific purposes of the processing of diagnostic data. The government organisations can successfully appeal to this ground for the keeping of audit log, as these data are necessary to comply with the legal obligation to keep logs of access to personal data, and being able to detect security incidents. As a joint controller, Microsoft may rely on this legal ground to provide this service to the Enterprise customers, but it may not use these audit logs or any other diagnostic data for other purposes than the same detection of unauthorised access, unless Microsoft is able to precisely document what other diagnostic data would be necessary for security purposes

b. MS and government Enterprise customers as (joint) controllers for the diagnostic data about certain discretionary Connected Services.

Microsoft mistakenly claims in its response to this DPIA report a legal obligation for the storing of all the diagnostic data about the discretionary Connected Services, in order to comply with GDPR security requirements. The use of Connected Services itself must indeed be adequately secured by Microsoft, but there is no obligation to store all diagnostic data for this purpose, including the contents provided by user when she uses for example the spelling service.

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*"

MS and government Enterprise customers as a (joint) controllers for all diagnostic data (incl. all mandatory Connected services)

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

Microsoft mistakenly claims in its response to this 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.

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.*"

MS and government Enterprise customers as a (joint) controllers for all diagnostic data

Both the Dutch government organisations and Microsoft may process a limited set of diagnostic data on the basis of necessity for their legitimate interest. This includes processing of diagnostic data to determine what security updates to serve, and to provide a well-functioning product by troubleshooting and technical error fixing. This does not include any of the other purposes for which Microsoft processes the diagnostic data.

In its GDPR compliance framework, Microsoft indicates that this legal ground would apply to all Event logging, and to 'Protection of log information' to ensure the security of the personal data.[155] In its response to this DPIA report, Microsoft claims that the greater public interest that is served by a secure Office ecosystem, prevails over the individual rights and freedoms of end-users. Microsoft claims: "*By being able to quickly react to security threats, Microsoft protects vital parts of infrastructure, government, business, communications and the public at large.*"[156] Even assuming that Microsoft would be able to fulfil such a role as global protector, Microsoft processes the diagnostic data for 8 purposes, not limited to security purposes.

Absent comprehensive documentation, it has to be assumed that diagnostic data may include both metadata about user behaviour, as well as content of the communication (at the very least, the sentences surrounding words that are searched in Bing or offered for spelling or translation). Both types of data can be very sensitive. Following the order of the Dutch government DPIA model, the necessity of the processing is separately assessed in section 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. Based on the requirements of article 5(3) of the ePrivacy directive (article 11.7a Tw in the Netherlands), 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. As analysed above, employees are not free to give consent for other purposes.

In sum, as joint controllers Microsoft and the government organisations cannot rely on consent given the dependency in the relationship between employees and employers. Employers may invoke the legal ground of compliance with a legal obligation to store and analyse the audit logs, to detect security incidents. But Microsoft may not use these data for its own purposes.

It is possible that a very limited set of data may be processed by both parties based on the necessity to perform a contract, or the necessity for a legitimate interest. But to successfully appeal to these legal grounds, transparency is essential. Absent comprehensive documentation, it has to be assumed that diagnostic data may include both metadata about user behaviour, as well as content of the communication. Both types of data can be very sensitive. This special character of the diagnostic data precludes further processing for most of the current purposes.

[155] Microsoft Compliance Manager Office 365, tab 'Customer Managed', items 6.9.3 and 6.9.4. 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

[156] Microsoft confidential response to this DPIA report, 24 September 2018, p. 17.

Illustration 7: table with the different applicable legal grounds in the current circumstances

Purpose	Legal ground	Joint controllers Government	Joint controllers Microsoft
Security (Audit log)	Consent	X	X
	Contract	√	X
	Legal obligation	√	X
	Legitimate interest	√	√
Updates	Consent	X	X
	Contract	√	X
	Legal obligation	X	X
	Legitimate interest	X	X
Troubleshooting and error fixing	Consent	X	X
	Contract	√	X
	Legal obligation	X	X
	Legitimate interest	√	√
Product development	Consent	X	X
	Contract	X	X
	Legal obligation	X	X
	Legitimate interest	X	X
Product innovation	Consent	X	X
	Contract	X	X
	Legal obligation	X	X
	Legitimate interest	X	X
General inferences / machine learning	Consent	X	X
	Contract	X	X
	Legal obligation	X	X
	Legitimate interest	X	X
Targeted recommendations	Consent	X	X
	Contract	X	X
	Legal obligation	X	X
	Legitimate interest	X	X
Compatible purposes	Consent	X	X
	Contract	X	X
	Legal obligation	X	X
	Legitimate interest	X	X
12 different purposes in Privacy Statement (only for the voluntary Connected Services)	Consent	X	X
	Contract	X	X
	Legal obligation	X	X
	Legitimate interest	X	X

12. 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. 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. There was no central rule against which an auditor could test if the existing or newly added events were legitimately added. Though it appears from the answer from Microsoft to this DPIA report that recently rules have been created, this does not apply to all the old events that are still included in the telemetry data. Therefore, Microsoft is unable to determine what personal data are processed for what purposes. Because of this lack of clear purposes, Microsoft has also so far been unable to inform data subjects about the personal data and purposes for diagnostic data.

Microsoft tries to cover this lack of purpose limitation with 3 broad purposes. But when questioned, there are at least 4 other purposes, plus any other purpose that Microsoft would deem compatible. That means these 3 broad purposes are not explicit nor specified.

As quoted in section 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 wants to present targeted recommendations on screen. This is one of the purposes which Microsoft deems compatible with the overall purpose of 'providing the service'.

This shows that the purpose and sub-purposes are too broad to demarcate what is permitted and what not, and what the *tenants* can expect, and what not. There is no limitation to the amount of sub-purposes that Microsoft may add. Given this lack of purpose limitation, nor the tenants nor Microsoft can trust that personal data will only be processed for legitimate purposes.

13. Special categories of personal data

As explained in section 2 of this DPIA, it is up to the individual Government organisations to determine if they process special categories of data, and if they wish to store special categories of data on Microsoft's computers (SharePoint or OneDrive). They should consider the risk that snippets of special categories of data could end up in system generated log files. In view of the analysis that Microsoft and that organisation are joint controllers for the diagnostic data, that processing would be prohibited. At first sight, there is no clear legal exception in the articles 9 and 10 of the GDPR, but this assessment must be conducted by the individual data controllers. The only general useful exception in article 9 GDPR is if the data subject has given explicit consent. Since nor Microsoft nor the tenants can obtain 'unambiguous' consent, they certainly can not meet the higher threshold of '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.

14. Necessity and proportionality

The principle of proportionality

The concept of necessity is made up of two related concepts, namely proportionality and subsidiarity. The personal data which is processed must be necessary to 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, these alternatives have to be used.

Second, proportionality demands a balancing between the interests of the data subject and the 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 less personal data, then the amount of personal data processed should be decreased to what is necessary. Therefore, essentially, the 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 therefore also closely related to the principles of data protection from article 5 GDPR.

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.[157]

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.

Absent any documentation from Microsoft or tool to inspect the telemetry data, the processing of diagnostic data is not transparent. The lack of transparency inherently makes the data processing unfair. The lack of transparency equally makes it impossible to assess the proportionality of the processing.

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 diagnostic data. Microsoft provides no choice at all with regard to the content and volume of Office telemetry data for either the tenant or the employee. The only setting regarding diagnostic data that is set default to OFF is the

[157] 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).*

collection of data '*to improve Office*'. The collection of the audit log is currently also switched OFF, but, as described in section 2.1, Microsoft plans to change this to default ON.[158]

Because Connected Services are switched ON by default, as soon as an employee uses such a service from within Office, Microsoft starts to collect an unknown amount of diagnostic data about the behaviour of the user. Nobody, not even Microsoft, knows what type of data are collected by the 23.000 to 25.000 types of events that are currently collected via the telemetry client; and there is no overview of other diagnostic data. The data are stored for 30 days up to 18 months, but this may also be forever, if Microsoft finds it necessary, or if an engineering team stores its own data subset separately. It is hard to argue that such old data are necessary, adequate and relevant. Especially because even Microsoft has lost overview, and does not know the reason for all events that once have been added but never deleted. Microsoft's rebuttal to this DPIA report, that it does practice data minimisation by sampling part of the telemetry data, does not change this conclusion.

In sum, possible usefulness (*nice to have*), does not meet the strict requirement of necessity. Some of these Connected Services explicitly collect content data, such as the line preceding and following a word or phrase to offer a grammar check, a translation, a search result, or to look-up data about that topic on the Internet. In view of this sensitive nature of the diagnostic data, the processing of diagnostic data by Microsoft disproportionately infringes on the interests and rights of the affected data subjects (the employees/workers, and all Dutch citizens that may be mentioned in government correspondence and documents).

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).

Though Microsoft has 2 different storage periods for the telemetry data, of 30 days and 18 months, Microsoft may store the data much longer, if it considers that to be necessary, or if an engineering team stores its own cube of data. Though Microsoft must necessarily collect both traffic and content data to deliver its services, the company should treat these data as functional data, and only process them for the duration of the transmission or provision of the requested result. Because it is technically easy and cheap to collect and store large amounts of data for 'you never know', that doesn't mean it is necessary, and thus, proportionate. Given the sensitive

[158] "*We're in the process of turning on auditing by default. Until then, you can turn it on as previously described.*" Source: Microsoft, Search the audit log, URL: https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

nature of diagnostic data, this factually unlimited storage is a disproportionate infringement on the rights and freedoms of all the different affected data subjects: employees and Dutch citizens.

Assessment of the subsidiarity

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

There are hardly any direct equivalent alternatives to Microsoft Office for most Dutch government organisations.

According to Microsoft, the purposes for which diagnostic data are processed in Office are completely up to the controller, as the *tenant* can choose whether or not to use the product, and determine the scope of the processing by selecting the settings. In reality, this freedom is 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 is no directly equivalent software alternative for the Dutch government. Alternative providers such as Google, or open source software such as Open 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.

If government organisations continue to use the Office software, and Microsoft does not make amends, these organisations should consider to switch to purely local, on-premise use of the 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

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

15. Rights of Data Subjects

The GDPR grants data subjects a number of rights. In the first place, the data subject has the 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 sections of this report, Microsoft provides no documentation about the Office diagnostics, nor in a technical language for admins nor in clear and plain language for employees or other data subjects whose personal data may be involved by this data

processing. This leaves the government organisations, as joint controllers, incapable of adequately informing their employees.

In the second place, the data subject has the right to access personal data concerning him or her. Upon request, the data subject must be informed whether personal data about him or her is processed by the controller. If this is the case, the data subject must be provided with a copy of the personal information which is the subject of the processing, along with information on the purpose of processing, recipients to whom data has been transmitted, the period for which personal data is to be stored, and information on the rights of the data subject. Microsoft engages to "*comply with reasonable requests by Customer to assist with Customer's response to such a data subject request*."[159] Furthermore, Microsoft states that when it acts as processor, it will redirect a request to the data controller.[160]

Microsoft provides a tool to admins 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).[161] Privacy Company has used the DSR tool provided by Microsoft. The obtained files provide information about the use of (cloud-only) Office 365. The files include 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 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 Services.

Thus, when a data subject exercises her rights under the GDPR, and requests access to her personal data, the answer via the DSR tool is exclusively based on the data that Microsoft qualifies as Customer Data. This may include associated data required by IT systems to function but that the user does not directly input, such as the content of the e-mail header defined in RFC 5322.[162]That a processor redirects requests of the data subject to the controller is in line with the system of the GDPR. However, this DPIA concludes that Microsoft and the *tenants* are joint controllers for the diagnostic data. Therefore Microsoft and SLM Rijk must agree as joint controllers how data subjects can exercise their rights, and get a complete list and explanation of personal data. Microsoft offers a very good automated tool for DSR, but the results of an access request should not be limited to some diagnostic data that Microsoft acknowledges to be personal data in the category of Customer Data

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 factually delete historical diagnostic data, except for deleting the user account completely. 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. Microsoft explains why it is not possible to

[159] OST September 2018, p. 8.
[160] OST September 2018, p. 8.
[161] Guidance is available at https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365
[162] Microsoft confidential answer 1 October 2018 to the 10 follow-up questions, answer Q6a.

delete individual historical diagnostic data, because they are a factual record of user actions and associated system performance in an ongoing relationship between a customer and Microsoft. Deletion of logs would have significant functional impacts, because features that rely on memory (ability to pick up work on another device), would not longer work.[163] 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.[164]

In the fourth place, employees have the right to object against a solely automated decision if it produces a legal effect. Employees are not able to object against a decision to include their device in a sample for the collection of additional telemetry data. Though this decision does not produce legal effects, and does not otherwise significantly affect the employees, this collection of additional telemetry data may cause extra risks for some employees. For example, if they regularly work with classified information the collection of extra data about their usage of the Office software may lead to increased risks of social engineering/spear phishing and even stalking.

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 section 11 of this report, the data processing for 3 purposes can be based on this legal ground, namely, for Security (Audit log), to provide Updates and for troubleshooting and error fixing. 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 tenants 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 recently formed coalition of USA based providers called the Data Transfer Project. This initiative includes Facebook, Google, Microsoft and Twitter.[165]

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.

[163] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, Answer Q4d.
[164] Idem, Answer Q4e.
[165] 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/

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

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

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

Both Microsoft and the government institutions are able to use the collected data about user behaviour in Office to distill a picture/create a profile of a person. 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 effective working hours, from first log-in to last log-out, and time spent with the different applications. 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 also be a risk of blackmailing and stalking for the employees. Additionally, employees 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 Microsoft 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."[166]

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."*[167]

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 a person might allow for an equally privacy-invasive detailed monitoring of an individual's life and behavioural patterns."*[168]

The DPAs also see a risk that employees no longer dare to report anomalies, which can undermine internal whistle-blowing schemes.[169]

There is an additional risk for some types of government employees if the metadata 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 further processing would be in breach of confidentiality requirements and the fundamental right to protection of communication secrecy. Such analysis may also breach government secrecy classifications.

[166] Article 29 Working Party (now: EDPB), WP 249, Opinion 2/2017 on data processing at work, p. 9-10.
[167] 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.
[168] WP 249, p. 10.
[169] Idem.

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 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 the metadata are stored disclosing information about this protected communication.

16.1.2 Content

Even though Microsoft has as a policy that diagnostic data should not include content, some system generated event logs do include content, such as the subject line of e-mails and titles of documents. Microsoft may also store and analyse sentences surrounding words for a variety of purposes that include 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 online 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.

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

Currently, Microsoft provides no documentation or data viewer tool for the Office telemetry data. There is limited documentation about the audit logs and system-generated event logs, but no information about the telemetry data. In the absence of information, the likelihood of the occurrence of all five risks is more likely than not, while the impact may range from minimal to serious harm.

16.2.2 Lack of control

Government organisations have no possibility to influence or end the collection of diagnostic data (no settings for telemetry levels). In the absence of control, the occurrence of all five risks is more likely than not, while the impact may range from minimal to serious harm.

16.2.3 Sensitive nature of the metadata and possibly content

The diagnostic data contain sensitive metadata about the individual use of the services and possibly content. Both types of data may contain highly sensitive or confidential data, but Microsoft does not acknowledge that all diagnostic data, including the telemetry data, are personal data. The processing of system generated event logs may lead to some impact (chilling effect on employees) and to serious harm (inability for data subjects such as detainees to communicate confidentially, risk of leaking of state secret information), while the likelihood of the risks of loss of control, loss of confidentiality, reidentification of pseudonymised data and unlawful further processing are more likely than not.

16.2.4 Microsoft does not act as a data processor

It follows from the factual analysis in this DPIA report that Microsoft cannot be qualified as a data processor. However, Microsoft does not accept its role as joint controller with the government organisations that use Office, as defined in article 26 of the GDPR, and as filled in by recent jurisprudence from the European Court of Justice. Even though Microsoft determines to a large extent what personal data will be processed through diagnostic data and for what purposes, Microsoft insists that it only acts as a data processor. This is legally incorrect. Since data processors are legally prohibited from determining the purposes of the data processing, and the government organisations are instrumental in enabling Microsoft to process the diagnostic personal data, Microsoft and the government organisations have to be qualified as joint controllers. The current contractual framework does not reflect the role of Microsoft as a joint controller for the processing of the Office diagnostic data. This incorrect contractual arrangement also extends to the processing of diagnostic data through some Connected Services for which Microsoft assumes it is (the only) data controller.

The incorrect qualification of roles in the framework agreement leads to a significant possibility of serious harm. This because of the lack of control for the government organisations over the purposes of the data processing, and thus a high risk of unlawful processing of data of employees and other data subjects. It also leads to a risk of reidentification of pseudonymised data, and to the risk of an incorrect division of tasks with regard to the exercise of data subjects rights).

16.2.5 Not enough control over sub-processors and factual processing

Even though Microsoft has attached quite some safeguards to the use of sub-processors, it is difficult for SLM Rijk and the individual government organisations that use Office to verify the integrity of these sub-processors itself and other types of processing, such as the processing of personal data in Cosmos. The audits organised by Microsoft examine the structure of rules and the existence of checks, but not how the data are factually processed.[170] In an amendment on the

[170] 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.

Online Service Terms, Microsoft hesitantly agrees to take a suggestion for other audit questions in consideration, but Microsoft has also indicated during the meetings with SLM Rijk and Privacy Company that Microsoft is not willing to give the Dutch government the same audit rights as for example the financial services industry in the Netherlands. In view of the fact that some sub-processors are content delivery networks that probably make real-time copies of all data, and many sub-processors are located outside of the EU, there is a reasonable likelihood that these sub-processors can process the diagnostic data for unauthorised purposes. There is also a significant possibility that the processing of historically collected telemetry data breaches the GDPR and thus causes harm.

Given the lack of information, and the lack of supervision through audits, and the fact that SLM Rijk cannot force Microsoft to stop the cooperation with one or more specific sub-processors, the risks must be assessed as reasonably likely to occur, while the possible harm must be qualified as serious.

16.2.6 No purpose limitation

Microsoft processes the diagnostic data from the Office Applications and the mandatory Connected Services for 7 purposes, and (8st purpose) for all other purposes that Microsoft deems compatible with those purposes. Microsoft does not allow the Enterprise customers to reject processing for specific purposes. It is, for example, not possible for government organisations to prevent Microsoft from using the diagnostic data to show targeted on-screen recommendations to use certain other Office services or tools. This lack of purpose limitation leads to a systematic loss of control (high likelihood of harm), as well as an inability to protect fundamental rights from employees and citizens such as the right to confidentially send and receive information, as well as the risk of a reasonable probability of reidentification of pseudonymised data.

Additional risks arise as a result of the use of discretionary Connected Services. Microsoft states in the privacy statement that when a person uses voluntary Connected Services, data will be shared with third parties, or with other subsidiaries of Microsoft. For instance, when a user uses the search service, one of the Connected Services, "*Office will send your requested word or phrase and some surrounding content from your document*"[171] . It is not clear for what period of time these data are stored, and for what purposes they are processed. Without further purpose limitation, it has to be assumed that Microsoft may process these data for the 12 broad purposes from its privacy statement.

The likelihood of unlawful (further) processing is 100%, as this report identifies that there is no legal ground for many of the current purposes for which Microsoft processes the diagnostic data. The severity of the impact depends on the content of the diagnostic data, and can vary between minimal impact to serious harm.

16.2.7 Indefinite retention period

The Office telemetry data are stored for 30 days up to 18 months in the central Cosmos database in the USA, but longer if Microsoft deems this to be necessary. 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

[171] Microsoft privacy statement under "Productivity and Communications Products", Office. https://privacy.microsoft.com/en-GB/privacystatement

diagnostic data, is by deleting the user account in Active Directory, and by creating a new account for that user.

The risks resulting from such a long or even indefinite retention period are per definition high. The GDPR requires organisations only store personal data as long as necessary, related to increased risks of unlawful processing, of incorrect data and of data breaches. In view of the assessment that historically collected diagnostic data may include highly sensitive personal data, the potential harm must be qualified as serious.

16.2.8 Processing of personal data outside of the EEA without adequate guarantees

The transfer of data is a risk in itself. As has been explained above, in the paragraph about the identification of the risks, diagnostic data reveal behavioural information about employees and other people in the Netherlands that communicate with these employees. The diagnostic data may also include parts of the content of documents when using Connected Services and subject lines from e-mails. This leads to a high risk of serious harm, especially when the collected data (inadvertently) include special categories of personal data, and classified information.

Though a narrow subcategory of content data provided to online services such a SharePoint, labelled by Microsoft as Customer Data, is stored within the European Union, other information is transferred to and stored in locations in other places around the world. It has to be assumed that Microsoft does not consider most diagnostic data to be part of the (protected category of) Customer Data. This movement of personal data outside of the European Union occurs on a daily basis (occurrence high) and entails the following risks:

a) The standard of protection of personal data in most countries in the world is lower than in the European Union. While Microsoft undertakes to ensure a uniformly high standard of protection, this protection cannot be guaranteed against government intervention of third countries. There is therefore an appreciable risk that information held by Microsoft in a data centre in a third country can be accessed by local governments.

b) Microsoft transfers the personal data from Office 365 ProPlus to the United States under the terms of the EU-US Privacy Shield Framework. Microsoft has self-certified under this regime.[172] However, there is some concern about the viability of the Privacy Shield. The terms of the Privacy Shield are expected to be reviewed soon and it is not certain if the agreement can remain in force.[173] It is up to the European Court of Justice to decide whether this type of agreement is sufficient mitigation for the risks of extensive surveillance.[174]

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

[173] See the letter from Commissioner Věra Jourová from 26 July 2018 to the Trump administration, URL: https://gdpr.report/news/2018/07/31/jourova-puts-trump-administration-on-notice-with-letter-to-america/. See also the motion from the European Parliament from 26 June 2018, URL: http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2018-0305&language=EN in which the EP concludes that *the current Privacy Shield arrangement does not provide the adequate level of protection required by Union data protection law and the EU Charter as interpreted by the European Court of Justice*;

[174] In case Case C-311/18 the European Court of Justice will take the facts into consideration established in the case of Max Schrems versus the Irish DPC. The Irish High Court held a trial in February and March 2017. On 3 October 2017, the court found that the DPC was correct to believe that the Standard Contractual

Microsoft also offers Standard Contractual Clauses (also called "Model Clauses"). These clauses, drafted by the European Commission in 2010, allow a non-EU company to receive data from the EU.[175] However, there are two problems with these clauses. First of all, Microsoft only applies these Clauses to the so called 'Core Services' (such as SharePoint and OneDrive), and not to Office 365 ProPlus installs. Secondly, even if the SCC apply, Microsoft only offers prefilled model clauses in the generic Online Service Terms, without a possibility for the Enterprise customer to negotiate individual details in the Annexes.

c) The recently adopted US American CLOUD act presents a risk for the personal data of employees of the government organisations. The cloud act essentially extends jurisdiction of the US American authorities to all data held by American corporations, even when that data is stored in data centres outside of the territory of the United States. As the documents processed by the Dutch government are especially vulnerable in this regard, access to this data should be considered an especially high risk.

16.3 Summary of Risks

These circumstances lead to the following high data protection risks:

1. No overview of the specific risks for individual organisations due to the lack of transparency (no data viewer tool, no public documentation)
2. No possibility to influence or end the collection of diagnostic data (no settings for telemetry levels)
3. The unlawful storage of sensitive/classified/special categories of data, both in metadata and in content, such as for example subject lines of e-mails
4. The incorrect qualification of Microsoft as a data processor, in stead of a joint controller as defined in article 26 of the GDPR
5. Not enough control over sub-processors and factual processing
6. The lack of purpose limitation both for the processing of historically collected diagnostic data and the possibility to dynamically add new events
7. The transfer of (all kinds of) diagnostic data outside of the EEA, while the current legal ground is the Privacy Shield and the validity of this agreement is subject of a procedure at the European Court of Justice
8. The indefinite retention period of diagnostic data and the lack of a tool to delete historical diagnostical data

Clauses (between Facebook Ireland and Facebook Inc in the USA) were invalid. The ruling from the High Court is available at: http://www.europe-v-facebook.org/sh2/HCJ.pdf.

[175] European Commission information page: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en

Based on the ICO model, this results in the following matrix:[176]

Severity of impact	Serious harm	Low risk	High risk 2 (employer)	High risk 1, 2 (MS), 3, 4, 5, 6, 7, 8
	Some impact	Low risk	Medium risk 5	High risk 1, 2, 7, 8
	Minimal impact	Low risk	Low risk	Low risk – only for innocent personal data 1, 2, 4, 5, 7, 8
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm (occurrence)		

[176] 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

Part D describes the proposed (counter-)measures. The following section discusses whether the proposed risk mitigating measures effectively counter the possible negative impact and risks connected to the processes in question.

17. Risk mitigating measures

Some risks described in this version of the DPIA may be mitigated by information from Microsoft. SLM Rijk should continue to work with Microsoft to obtain further answers from Microsoft to the (long) list of questions. Though Microsoft has answered a follow-up list of 10 questions related to the initial response of Microsoft to the facts in this DPIA, the list of 100 initial questions as a result of the meetings with Microsoft remains to be answered. Some future answers may lead to a different appreciation of the data protection risks.

Currently, the two only realistic measures that government organisations may take to reduce at least one of the risks described in section C, is to apply the new zero-exhaust settings to minimise the telemetry and to centrally prohibit the use of the voluntary Connected Services. SLM Rijk will commission a follow-up DPIA to test whether the zero-exhaust settings function properly. Additionally, government organisations should refrain from switching to the web-only version of Office 365 until more clarity has been provided by a follow-up DPIA and by Microsoft about the contents, purposes and impact of the processing of diagnostic data.

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.[177]

17.1 Announced risk mitigating measures

Microsoft has committed to publish documentation about the Office telemetry data and to offer new granular telemetry choices for Office admins. Microsoft has also committed to develop a data viewer tool in Office for the Office telemetry data.

In the interim, Microsoft has provided the Dutch government with zero-exhaust settings to minimise the processing of telemetry data, based on the blocking of traffic from certain ports that send information to the telemetry end-point in the USA. Such a solution has already been provided confidentially in 2013 with regard to Office 2013. The effectivity of this solution has to be tested in combination with the future new data viewer tool. The results of this inspection will be the subject of a follow-up DPIA.

Microsoft has not agreed to any of the following risk mitigating measures to reduce the data protection risks:

- M3a Offer a possibility to delete historical telemetry data based on device ID

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

- M3b Guarantee not to store content data in future telemetry and other diagnostic data unless strictly necessary (such as subject lines in system generated event logs)
- M4a Redefine purposes to fit with a data processor role[178], or acknowledge joint controllership in a new Framework agreement as defined in Article 26 GDPR and include the processing of diagnostic data through all Connected Service in the scope of the (new) joint controller agreement
- M4b Only process data from (voluntary) Connected Services as a data processor or change the default setting for Connected Services to 'Off'
- M5 Allow government to collectively add new audit questions
- M6 Limit the purposes for which the diagnostic data may be processed to the strictly necessary purposes for which the government institutions have a legal ground.
- M7 Develop a GDPR compliant transfer agreement between joint controllers and/or store audit logs and other diagnostic data only in EU data centres
- M8 Determine the necessary retention periods for different types of diagnostic data

17.2 Residual risks

Some residual risks can be mitigated if the government organisations will use the newly developed settings to minimise the processing of telemetry data.

Assuming Microsoft will be offering a data viewing tool and assuming Microsoft will provide global solutions to the risks of the lack of transparency and ability to control the level of telemetry collection, the first two risks will be mitigated by the measures Microsoft has currently committed to take.

Government organisations must exert every effort to mitigate these high risks, amongst others by centrally prohibiting the use of the voluntary Connected Services and the option for users to send personal data to Microsoft to 'improve Office'. They should refrain from using the SharePoint/OneDrive online storage, and delay switching to the web-only version of Office 365 until Microsoft has provided adequate guarantees with regard to the types of personal data and purposes of the processing.

Additionally, the *tenants* should consider the following additional measures:

- Periodically delete the Active Directory account of some VIP users, and create new accounts for them, to ensure that Microsoft deletes the historical diagnostic data
- Consider using a stand-alone deployment without Microsoft account for confidential/sensitive data
- Conduct a pilot with alternative software, after having conducted a DPIA on that specific processing This could be 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.[179]

[178] That is, process the diagnostic data only for purposes for which government organisations have a legal ground.
[179] Kamerstukken II, 2010-2011, 32 679, Open standaarden en opensourcesoftware bij de rijksoverheid.

The risks and possible risk mitigating measures can be visualised in the following table. The lines printed in italics are measures Microsoft has not agreed to.

Nr	Risk	Possible measure Microsoft	Possible measure per tenant
1	Lack of transparency	Public documentation and data viewer tool	Use tool when it becomes available
2	No possibility to influence or end the collection of telemetry data	a. Temporary settings to minimise the processing	Use temporary minimisation settings
			Do not use SharePoint/OneDrive
			Do not use web-only Office 365
		b. Permanent settings for telemetry levels	Use setting telemetry Off when switch is available
3	Unlawful collection and storage of sensitive/ classified/special categories of data	*a. Option to delete historical diagnostic data by Device ID*	Consider deleting some specific users and creating new accounts for them
		b. Guarantee never to store content data in telemetry data or in other system-generated event logs unless strictly necessary	Prohibit users from sending personal data to Microsoft to 'improve' Office
			Consider pilot with other software for some functionality (after conducting a separate DPIA)
4	Incorrect qualification Microsoft as data processor	*a. Minimisation of purposes to be able to act as a processor OR New framework agreement as joint controller*	Endorse new framework agreement as processor or joint controller
		b. Only process data from voluntary Connected Services as a data processor OR change default for voluntary Connected Services to 'Off'	Prohibit voluntary Connected Services unless Microsoft offers these services as a processor
5	Not enough control over sub-processors and factual processing	*More audit rights*	Consider stand-alone deployment without Microsoft account for confidential/sensitive data
6	The lack of purpose limitation	*Processing only for strictly necessary purposes for which the tenants have a legal ground*	- no specific measure, see above
7	The transfer of data outside of the EEA	*New contractual guarantees and/or storage of diagnostic data within the EU*	- no specific measure, see above
8	The indefinite retention period of diagnostic data	*Determine necessary retention periods*	- no specific measure, see above

Conclusion

Given the ongoing negotiations with Microsoft (and Microsoft's written commitments as a part of these negotiations) to mitigate the remaining risks, SLM Rijk postpones consultation of the Dutch data protection authority for risks 3 - 8.

ANNEX 1 – Description of key functionalities in Office

Microsoft Word

Microsoft Word is a popular word processor, a programme used for text editing and creating written documents. Word is widely used in the daily work of most if not all government organisations. Almost all members of the staff will work in word documents daily.

Microsoft Excel

Microsoft Excel is a programme for spreadsheets. It features among other things tables, calculation, and graphics. Microsoft Excel is likely used by most if not all government organisations. Depending on the tasks of a specific employee, this programme might be used daily or occasionally.

PowerPoint

PowerPoint is a software programme with which users can create visual support for presentations. It allows the creation of a series of sheets that can be used to visually display information. It is likely that most if not all employees of government organisations use PowerPoint when they give presentations.

Outlook and Calendar

Outlook is a suite of tools for the management of personal information. While Outlook contains a range of different tools, the most widely-used tools are the email application and the calendar. Both of these applications are used daily in the work of all of the employees of governmental organisations.

Connected Services

All of the programmes which are part of Office are supplemented to some extent by Connected services. Connected services, also called Intelligent Services by Microsoft, are features that make use of a remote connection to fetch extra information from Microsoft servers for the user. The third column specifies how Microsoft sees its own role; as controller or data processor.

3D Maps	3D Maps for Excel is a three-dimensional data visualization tool that provides information and insights that may not be available in traditional two-dimensional tables and charts. Excel data that has geographic properties in table format or in a Data Model—for example, rows and columns that have names of cities, states, counties, zip codes, countries/regions, or longitudes and latitudes are best suited for 3D Maps.	Controller
Editor	Editor gives you an overview of errors found in your document and lets you choose which ones you want to fix. Editor spots misspellings, grammatical mistakes, and writing style issues and marks them as you	Controller

	type: red squiggles for spelling, blue double underlines for grammar, and gold dotted lines for writing suggestions.	
Bing (Weather)	Weather on the Calendar surface	Controller
Giving Feedback to Microsoft	Feedback features include Send-a-Smile in Office desktop for Windows, Help Improve Office in Office desktop for Mac, and Give Feedback to Microsoft in Office Online. These features all let you send feedback to Microsoft about your experiences in Office ProPlus Applications. You can submit positive, or negative, written feedback or suggestions. You can choose to send a screenshot and/or your email address which will only be used to contact you for follow up related to your feedback	Controller
Insert 3D Models	You can insert rotatable 3D models into Word, Excel and PowerPoint on Windows, based on your chosen subject. 3D Models inserted from online sources are sourced from Microsoft Remix 3D, using Bing to search for relevant models.	Controller
Map Chart	Map Chart in Excel helps you to create and insert a customized map and charts specific to your data set. The data set is sent to Microsoft and, using Bing, a suggested map or chart is returned. Map Chart can include geographical representations of your data, and data counts, for: countries, regions, states, counties or postal codes.	Controller
Office Help and Quick Starts	Microsoft creates and publishes help experiences. It provides self-help articles and videos, called Quick Starts, on how to troubleshoot and use Office. If you choose to let Office connect to online services, content may be viewed in an in-app experience in any Office application. Also, Tell Me can connect you to Office Help articles and videos based on the search query you enter.	Controller
Office Store	Office Store is where you go to get add-ins—mini applications that extend what you can do with Office, Office 365, and SharePoint (2013 and 2016). For example, with Office add-ins you can use Wikipedia without leaving Word or get directions and maps right in Outlook. Addins are available for Access web apps, Word, Excel, Outlook, Project, PowerPoint, and SharePoint.	Controller
Office Templates	You can download free, prebuilt, document templates from Office by clicking File > New in any Office app page Templates can include calendars, business cards, letters, cards, brochures, newsletters, resumes, and so on. Templates can be customized to meet your needs. When you select a template, a dialog box is presented that shows a larger view of the template. To download and use it, click the Create button and a new file will be created using that template.	Controller
Online Pictures	Online Pictures provides access to search engines such as Bing, third-party providers such as Pixels, and your personal OneDrive, to search for pictures. Your search query is sent to the search engine you choose to provide this service. Microsoft Forms provides an Insert Image feature that lets you insert an image from a Bing search directly into your form.	Controller
Online Video	Online Video provides access to YouTube, and your personal OneDrive, to search for videos. In addition, you can enter a specific video embed code to retrieve a video from YouTube to insert into your file.	Controller
PowerPoint Quickstarter	QuickStarter builds a PowerPoint outline based on the subject you provide. This subject is sent to Bing as a search query and is used to find suitable images and text.	Controller
Researcher	Researcher in Word helps you find topics and incorporate reliable sources and content for your research paper in just a few steps. You can explore and research the material related to your content then add it with citations in the document without leaving Word	Controller

Resume Assistant	When you open a resume document, the LinkedIn Resume Assistant task pane opens. If you want to tailor your resume to a particular role or company, you can choose to receive a set of LinkedIn-powered examples and suggestions. Once your resume is complete, you will be given an opportunity to post it to LinkedIn.	Controller
Smart Lookup	By selecting a word or phrase and launching Smart Lookup, the selected text is sent to Bing as a search query, which provides more information, definitions, history and other resources from multiple thirdparty sites related to that word or phrase. You can select specific results to visit those sites directly.	Controller
Translator	Transmits a highlighted word or section of user text, as well as a few words from either side of that text, to perform the requested translation. You might see a list of several translations and can expand the translated item to show a usage example in both languages.	Controller
Dictate	Dictate is an online service that will convert your speech as you talk to text in your document. Your speech utterances will be sent to Microsoft to provide you with this service.	Controller
3S Search	Mailbox search capabilities	Processor
Auto Alt-Text	Alt-text helps the user tag images in their document with text to be read to users with accessibility needs. The image is sent to a Microsoft service and a suggested descriptive text string is returned.	Processor
Binary File Conversion Service (BCS)	An online service that will convert files from Windows for Word, Excel and PowerPoint to be available on different platforms, including Mac, iOS, Cand Android	Processor
Data Types	(Yellow) Stock and geographic data in Excel is available by typing text into a cell, and converting it to the **Stocks** data type, or the **Geography** data type. These two data types are considered *linked data types* because they have a connection to an online data source that provides rich information.	Processor
HelpShift (Contact support)	Used to manage tickets when a user requests support via Outlook in-app support	Processor
Insights in Excel	Users can get fast, automated, insightful analysis about their Excel data by clicking a cell in a data range, and then clicking the Insights button on the Insert tab. Insights in Excel then analyzes the selected data and returns interesting visuals about it in a task pane.	Processor
Most Recently Used Documents	Microsoft Office programs display the last few documents a user has opened in that program so that the user can use those links to quickly access the files. This feature is turned on by default, but a user can turn it off, turn it back on, clear, or adjust the number of files that it displays.	Processor
Office Licensing Services	The user's Azure Active Directory (AAD) or Microsoft Account identifier is sent to an online service that compares against subscription purchase records to understand what the user is entitled to use, including the product licensed, type of subscription and the term.	Processor
Outlook Diagnostic Service	Provides on-demand diagnostics for Outlook (including Contact Support)	Processor
Print Service	Part of the Binary file Conversion Service that calls the iOS or Android native print service for word, Excel and PowerPoint printing on those platforms	Processor
PowerPoint Designer	PowerPoint Designer improves slides for Office 365 subscribers by automatically generating design ideas to choose from. While a user is putting content on a slide, Designer works in the background to match	Processor

	that content to professionally designed layouts.	
Roaming	The Office Roaming Service helps keep a user's Office settings up to date across devices running Office. When a user signs into Office with a Microsoft account or an account issued by that user's organization, the Office Roaming Service is turned on and syncs some customized Office settings to Microsoft servers (such as a list of most recently used documents and the last location viewed within a document). When that user signs into Office on another device with the same account, the Office Roaming Service downloads the user's settings from Microsoft servers and applies them to the additional device. The Office Roaming Service also applies some of the user's customized Office settings when signing into Office.com. When the user signs out of Office, the Office Roaming Service remove that user's Office settings from the device. Any changes the user made to customized Office settings are sent to Microsoft servers.	Processor
Rights Management Service	Software to help protect access to and usage of information flowing through mail applications that use rights management services (services that limit viewing, editing and distribution rights in mail applications)	Processor
Visio Online	Shape Search Diagrams and shapes available from Visio online through a user query in the Diagrams Made Simple search box. Returns diagrams and shapes from Visio Online based on the query.	Processor