Ministerie van Justitie en Veiligheid

DPIA Windows 10 Enterprise v.1809 and preview v. 1903

Data protection impact assessment on the processing of diagnostic data

Version 1.5

Date	11 June 2019
Status	public

Colofon

DPIA by

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

Contact

Paul van den Berg
E p.j.van.den.berg@minvenj.nl
T 00 31 70 370 79 11

Project Name

DPIA report diagnostic data processing in Microsoft Windows 10 Enterprise

Authors

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

Contents

Figures and tables

Summary

This report, commissioned by the Microsoft Strategic Vendor Management office (SLM Rijk) of the Ministry of Justice and Security, is a general data protection impact assessment (DPIA) on the processing of personal data related to the use of the Windows 10 Enterprise operating system. This report assesses the data protection risks for data subjects that may result from the collection of information about the use of Windows 10 Enterprise version 1809, released by Microsoft in the autumn of 2018. This report takes improvements into account introduced in version 1903, released end of May 2019. The report has been written by the Dutch privacy consultancy firm Privacy Company.

Scope: telemetry data at the Security level and Timeline
This report assesses the data protection risks for data subjects caused by the collection by Microsoft of telemetry data. Technically, Microsoft Corporation systematically collects diagnostic data about the individual use of the Windows 10 software (not limited to the Enterprise version). Via the in-built telemetry client, Microsoft automatically collects telemetry data on the device, and regularly sends these to its cloud servers in the USA.

Administrators can minimise this data collection by setting the telemetry level to Security, or block traffic to telemetry endpoints in the Microsoft cloud. The risks of data processing at higher levels of telemetry (Basic and Ful telemetry) are out of scope of this DPIA, because it follows from Microsoft's public documentation that at these levels, Microsoft can collect confidential or sensitive personal data.

Generally, government organisations store the content they produce with the Office software in governmental data centres, *on-premises*. This DPIA also assesses the risks of hybrid deployments, with data stored in SharePoint Online/OneDrive for Business.

This report also addresses the new Timeline functionality that allows users to synchronise activities on multiple devices via the Microsoft cloud.

No high data protection risks
Depending on the telemetry settings, the use of the Windows 10 operating system on the work computers may result in infringements on the right to data protection of government officials. These risks are a result of Microsoft's systematic collection of data about the use of its software and online services (diagnostic data). These diagnostic data are generally personal data.

Based on a technical analysis of the telemetry data traffic, this report concludes that at the Security level, Microsoft processes very little, and no sensitive personal data with the Windows 10 telemetry data. Therefore, with the telemetry set to Security, or if traffic to telemetry endpoints is blocked, there are no high data protection risks for data subjects.

This report identifies 4 low data protection risks caused by the diagnostic data processing in Windows 10 Enterprise at the Security level, assuming Windows Timeline is disabled. These risks are:

1. Lack of purpose limitation and legitimate basis for the diagnostic data processing

2. Lack of control over third parties/processors and audit questions factual processing
3. The transfer of (all kinds of) diagnostic personal data to the USA, while there are two procedures pending at the European Court of Justice questioning the adequacy of data protection guarantees.
4. The long retention period of diagnostic personal data

GDPR compliance and umbrella DPIA
The Windows 10 software is deployed on a large scale by different governmental organisations in the Netherlands, such as ministries, the judiciary, the police and the taxing authority. Approximately 300.000 government employees work with the operating system on a daily basis, often in combination with Microsoft Office software.

The Microsoft Strategic Vendor Management office (SLM Rijk) conducts negotiations with Microsoft for the federal government, but the individual government organisations buy the licenses and determine the settings and scope of the processing of diagnostic data by Microsoft Corporation in the USA. This general umbrella DPIA provides a guiding and corrective framework and is meant to help the different government organisations with the DPIAs they must conduct. This report cannot replace the specific risk assessments the different government organisations must make related to their specific deployment, the level of confidentiality of their work and the types of personal data they process.

Windows 10 Enterprise diagnostic data
Microsoft has explained that it collects circa 1.200 types of events via Windows 10 telemetry. These data are analysed by circa 10 Microsoft engineering teams. The collection of telemetry data is dynamic. Microsoft engineers can add new types of events to the telemetry stream without prior notice to the users. The Windows 10 telemetry data stream sent to the Microsoft servers in the United States is separate from, and independent of, the telemetry data stream generated by Microsoft Office. The streams are sent to different network endpoints.

In addition to the telemetry data, Microsoft also collects data on its own cloud servers when users access SharePoint Online and OneDrive (in system generated event logs). This data collection is invisible to end-users. In this report, both the telemetry data and the system generated event logs are referred to as 'diagnostic data'.

Microsoft correctly explains that diagnostic data should not be confused with functional data that necessarily have to be exchanged over the Internet to provide a requested functionality. For example, a local weather or news app may request a user's location. In that case, the location data are functional data. Therefore, the term diagnostic data refers to the separate registration at an individual level of technical metadata by Microsoft from and about the use at an individual level of the Windows 10 Enterprise software, and the use of cloud services such as SharePoint Online.

Technical analysis of the telemetry data
This report provides an analysis of the contents of the telemetry data as collected in the test lab by SSC-I, an IT-supplier that is part of the Dienst Justitiële Inrichtingen (the Custodial Institutions Agency). SSC-I has created this test lab for the Ministry of Justice and Security (hereinafter: the test lab). With the help of the Diagnostic Data Viewer in Windows 10 version 1809 and recording of traffic with Fiddler, the lab has recorded the outgoing traffic during, and for 3 days after, the performance of four minutely documented scenarios simulating the daily work tasks of an average government employee. These scenarios include the use of Windows Timeline.

Personal data
At the Security telemetry level Microsoft collects some information about the individual use by a government employee of the Windows 10 software. The collected telemetry data contains several unique identifiers. These identifiers allow Microsoft to combine information about the actions of a single user over time. Microsoft has the technical means to identify the individual user. Therefore, even though Microsoft collects very few data at the Security level, the collected telemetry data are personal data as defined in Article 4(1) of the GDPR.

During this assessment, at the Security level no user content (from files or emails) was observed in the Windows 10 diagnostic data flow.

Microsoft as a data controller
Microsoft incorrectly qualifies itself as (an independent) data controller for the data processing via Windows 10 Enterprise. Microsoft only qualifies itself (in its Online Service Terms) as a data processor for Windows Analytics and Windows Defender Advanced Threat Protection.

This legal position from Microsoft is different from other online services such as Azure and Office365, where Microsoft does qualify itself as a data processor. None of the contractual guarantees that have been agreed in the government enrolment framework apply to the processing of diagnostic data in Windows 10. Instead, only the consumer-oriented assurances from the general privacy statement apply.

A factual analysis shows that it is desirable that Microsoft would behave as a data processor. This is not the case in the current relation. Because Microsoft determines the purposes, and the government organisations enable Microsoft to process personal data, they are factually joint controllers for the diagnostic data processing. This relationship has not been formalised in a joint controller agreement.

Lack of purpose limitation and legal ground
In its technical documentation, Microsoft mentions specific purposes for the processing of diagnostic data about the individual use of its Windows 10 software. This information is not legally binding. Contractually, Microsoft can process the diagnostic data for almost all, broadly defined, purposes from its general privacy statement. The 16 relevant purposes include the use of personal data for personalised advertising in Windows 10 and in apps, to present commercial offers, and to use the contact data for promotional communications via email, SMS, physical mail and telephone.

The processing of the diagnostic data for so many broad and unspecific purposes violates the principle of purpose limitation.

An organisation may only process personal data if it has a legal ground for it. The possible legal grounds are summed up in Article 6 of the GDPR. Microsoft as (sole) data controller cannot rely on consent of employees, while such consent is necessary based on Article 11.7a of the Dutch Telecommunications Act for the retrieval of data over the internet via in-built software if the processing is not strictly necessary.

As a joint data controller, or as a data processor, Microsoft and government organisations may process a limited set of diagnostic data to determine what security updates to serve, to configure the telemetry pipeline, to detect and remove malicious software and to apply Windows Defender anti-virus and endpoint security protection.

If the purposes would be limited to these legitimate purposes, Microsoft could appeal to the legal grounds of the necessity for its own legitimate interest or that of the government organisation, and (in some cases) the necessity for the performance of the contract with the employee by the government organisation.

Conclusions
If government organisations follow the recommendation from SLM Rijk to use Windows 10 Enterprise only with the lowest level of telemetry, the Security level (or disable telemetry traffic), and prevent users from syncing their activities via the Windows Timeline, there are no high data protection risks resulting from the diagnostic data collection in Windows 10 Enterprise.

This report identifies contractual, technical and organisational measures Microsoft and the government organisations can take to completely remove the remaining low risks.

On 21 May 2019, Microsoft has released version 1903 for Windows 10 Enterprise. This version enables organisations to use Windows Update for Business functionality when the diagnostic data level is set to Security. In previous versions, this functionality was only available at the telemetry level Basic or higher.

SLM Rijk is providing significant input to Microsoft for an upcoming structural solution for Windows 10 Enterprise customers which is being designed for Windows 10 Enterprise 1809 and later versions. This will allow government organisations to have a simplified compliance solution for Windows 10 Enterprise at diagnostic data levels above Security. This solution will be ready in the foreseeable future, and Microsoft plans to make an announcement about this structural solution later this year.

Introduction

This report, commissioned by the Microsoft Strategic Vendor Management office (SLM Rijk) of the Ministry of Justice and Security, is a general data protection impact assessment (DPIA) on the processing of personal data about the use of the Windows 10 Enterprise operating system. This report assesses the common data protection risks for data subjects that may result from the use of Windows 10 Enterprise version 1809, released by Microsoft in the autumn of 2018. [1] This report takes into account an important improvement released in version 1903, the update distributed on 21 May 2019,[2] the ability to use Windows Update for Business when the telemetry level is set to Security.

The Windows 10 software is deployed on a large scale by different governmental organisations in the Netherlands, such as ministries, the judiciary, the police and the taxing authority. Approximately 300.000 government employees work with the operating system on a daily basis, often in combination with Microsoft Office software.

Ongoing GDPR compliance of different Microsoft products and services
SLM Rijk assesses the risks for all Microsoft products and services that are commonly used by government organisations, such as Windows, Office, Dynamics and Azure and approaches the risk mitigating measures with a holistic view.

Microsoft releases new versions of its Windows Enterprise and Office ProPlus software twice per year. As part of its ongoing commitment to ensure GDPR compliance, SLM Rijk intends to regularly commission new DPIAs on new versions of Windows 10 and Office 365, to guarantee the rights of data subjects on ongoing basis. New DPIA's can be necessary to examine the risks of changes in the technology and processing methods, to take account of modifications of the applicable laws and/or relevant jurisprudence, and to assess changes in the contractual agreement with Microsoft,

Previously, SLM Rijk has published a DPIA on the data protection risks of the autumn 2018 versions of Microsoft Office ProPlus (the locally installed versions of Office 2016 and Office 365).[3] SLM Rijk has commissioned a new DPIA report with an analysis of the data processing in the new April 2019 versions of Office ProPlus 2019 and Office 365 CTR, and has also commissioned DPIAs on the data processing risks of using Microsoft's Azure cloud services and Microsoft Dynamics.

Microsoft has been working constructively with SLM Rijk during the review of the risks of the use of these products, and has made major improvements to lower the data protection risks in Office 365 ProPlus in the new 1904 Spring version. Microsoft has

[1] The roll-out of Windows 10 Enterprise took place on 13 November 2018, see Microsoft IT Pro Blog, Windows 10, version 1809 rollout resumes; now available on VLSC, URL: https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/Windows-10-version-1809-rollout-resumes-now-available-on-VLSC/ba-p/284217 (URL last visited and recorded on 20 March 2019).

[2] Microsoft Windows Blog, How to get the Windows 10 May 2019 Update, 21 May 2019, URL: https://blogs.windows.com/windowsexperience/2019/05/21/how-to-get-the-windows-10-may-2019-update/ (URL last visited and recorded on 5 June 2019).

[3] This Office ProPlus DPIA report was published on 7 November 2018, with an update on the negotiations between the Dutch central government and Microsoft about the GDPR compliance. See: https://www.rijksoverheid.nl/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office (URL last visited 20 March 2019)

for example published a blog about the improvements[4], has introduced a switch to choose between the telemetry levels[5], has published new information about the contents of telemetry data[6], has enabled administrators to view the contents of the telemetry data with the same data viewer tool they can already use to inspect the contents of the Windows 10 telemetry stream[7], and has limited the purposes for the processing of data of some of the most widely used Connected Services such as the translation module (Translator) and the spelling checker (Editor).[8]

This DPIA report differs from an earlier DPIA report commissioned by SLM Rijk in the spring of 2018 about the diagnostic data flow from Windows 10 Enterprise. This previous DPIA report was written by the Dutch privacy consultancy firm Privacy Management Partners and delivered in June 2018. This previous report (not published) provides a risk assessment and recommendations to mitigate the data protection risks for (the previous version of) Windows 10 Enterprise.

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.[9] Different from that DPIA, this DPIA contains an analysis of the diagnostic data flow from Windows 10 Enterprise, with the help of the newly included Data Viewer Tool.

Umbrella DPIA versus individual DPIA's
SLM Rijk acts as a representative for the individual government organisations that procure and use the Microsoft Enterprise software. SLM Rijk is in the best position to

[4] Microsoft blog, Increasing transparency and customer control over data, 30 April 2019, URL: https://blogs.microsoft.com/on-the-issues/2019/04/30/increasing-transparency-andcustomer-control-over-data/ (URL last visited and recorded on 5 June 2019).
[5] Microsoft, Overview of privacy controls for Office 365 ProPlus, 8 May 2019, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/overview-privacy-controls (URL last visited and recorded on 5 June 2019).
[6] Microsoft, Required diagnostic data for Office, 16 May 2019, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data (URL last visited and recorded on 5 June 2019).
[7] Microsoft Office Support, Using the Diagnostic Data Viewer with Office (no date provided), URL: https://support.office.com/en-gb/article/using-the-diagnostic-data-viewer-with-office-cf761ce9-d805-4c60-a339-4e07f3182855?ui=en-US&rs=en-GB&ad=GB (URL last visited and recorded on 5 June 2019).
[8] Microsoft docs, Connected experiences in Office, 29 April 2019, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/connected-experiences (URL last visited and recorded on 5 June 2019).
[9] See the press release of the Dutch Data Protection Authority, 13 October 2017, Microsoft breaches data protection law with Windows 10, URL: https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-microsoft-breaches-data-protection-law-windows-10. A summary in English of these findings is available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/public_version_dutch_dpa_informal_translation_summary_of_investigation_report.pdf (URL last visited and recorded on 20 March 2019). The original report of findings, in Dutch only: AP, Rapport definitieve bevindingen Microsoft Windows 10, De verwerking van persoonsgegevens via Telemetrie -met correcties 6 oktober 2017-, URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/01_onderzoek_microsoft_windows_10_okt_2017.pdf (URL last visited and recorded on 20 March 2019)

negotiate improvements to lower the overall data protection risks that apply to the use of Microsoft software as used in governmental organisations. However, this umbrella DPIA cannot specifically determine what actual risks the processing involves for specific data subjects whose data are processed by the different government organisations. 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.

Windows 10 Enterprise diagnostic data

Technically, Microsoft Corporation systematically collects diagnostic data about the individual use of the Windows 10 software (not limited to the Enterprise version). Via the in-built telemetry client, Microsoft automatically collects telemetry data on the device, and regularly sends these to its servers in the USA. Microsoft has explained that it collects circa 1.200 types of events via Windows 10 telemetry. These data are analysed by 10 Microsoft engineers.[10]

A typical telemetry event contains a unique number, a timestamp, several unique identifiers for the end-user and the device, and different bits of information about for example the hardware that is used, the screen size, operating system, applications installed and usage details, as well as reliability information on device drivers.

Following the investigation by the Dutch DPA into the Windows 10 telemetry data in 2017, Microsoft has published extensive documentation about the Windows telemetry data and offers a Diagnostic Data Viewer in all Windows 10 versions. This tool allows end-users and administrators to inspect the diagnostic data that are collected on the device.

Microsoft correctly explains that diagnostic data should not be confused with functional data that necessarily have to be exchanged over the Internet to provide a requested functionality. For example, a local weather or news app may request a user's location. In that case, the location data are functional data.[11] Therefore, the term diagnostic data refers to the separate registration of technical metadata by Microsoft from and about devices with Windows 10 Enterprise through the Universal Telemetry Client. This includes data about inking and typing.

The Windows 10 telemetry data stream sent to the Microsoft servers in the United States is separate from, and independent of, the telemetry data stream generated by Microsoft Office ProPlus. However, if Windows telemetry is set to full, through the Windows telemetry, Microsoft can also collect rich event information about the use of Office applications such as Word, Excel, Outlook or PowerPoint.

Scope: Security level and telemetry disabled

Microsoft offers two telemetry settings for end-users in the different Windows 10 versions, **Basic** and **Full**. In the Windows 10 Enterprise version, the IT-pro's (the

[10] See the DPIA report commissioned by SLM Rijk on Microsoft Office ProPlus. Microsoft is quoted: "*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.*" Source: Meeting report 28 August 2018, answer to Q1.

[11] Microsoft, Windows IT Pro Center, Configure Windows diagnostic data in your organization, 4 April 2018, URL https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization (URL last visited and recorded on 5 June 2019).

administrators of the Enterprise version) can choose the minimum **Security** level or **disable** the diagnostic dataflow to known network endpoints.

This report describes the differences in data protection risks for data subjects between the lowest levels of telemetry settings: Security and telemetry disabled. In this second scenario all traffic to known telemetry endpoints to the Microsoft cloud is blocked. The risks of data processing at the Basic and Full levels of telemetry are outside the scope of this DPIA. This DPIA only addresses the telemetry at Security level, and a configuration where telemetry is disabled, to provide a technical assessment of the recommendation from the previous DPIA to switch the telemetry level to Security in order to minimise the data protection risks for data subjects.

The scope of this DPIA also includes the use of SharePoint Online and OneDrive and use of the Timeline functionality. The exact scope is explained in paragraph A1.2 of this report.

Technical analysis of the telemetry and Timeline data
This report provides an analysis of the contents of the telemetry data as collected by the test lab created by SSC-I for the Ministry of Justice and Security in December and January 2019 from Windows version 1809.[12] In close dialogue with Privacy Company, the technical lab has performed four minutely documented scenario's on virtual machines running Windows 10 Enterprise software version 1809.

The scenarios represent the collection of diagnostic data for the Security and disabled telemetry settings, both executed with an *on-premises* Active Directory and with a Hybrid Active Directory. In this latter hybrid network test, the cloud sync functionality of Timeline was switched On.

The technical lab relied on Microsoft's Diagnostic Data Viewer to inspect the outgoing telemetry. As an essential security measure, Microsoft encodes the outgoing traffic to its own servers in a way that makes inspection of the content of the traffic impossible with normal proxy-techniques. The technical lab recorded all outgoing network traffic with Fiddler. This setup ensures that any unexpected network traffic would be noticed. However, the use of Fiddler also blocked the functioning of some pre-installed apps such as Mail, Weather and News, and blocked traffic to Office applications in the hybrid deployment. All the captured outgoing traffic has been stored and provided in csv format to Privacy Company. Additionally, the lab has recorded all settings and actions on virtual disk images and has stored these images to be able to reproduce all actions and resulting telemetry events.

The details of the executed scenario's and main findings from the technical investigation are described in part A of this DPIA. Privacy Company has compared the results with the publicly available documentation from Microsoft about the Windows 10 telemetry data. Privacy Company has also studied the results of the detailed technical telemetry analysis conducted for the German Federal Office for Information Security (BSI), released 20 November 2018.[13]

[12] Dienst Justitiële Inrichtingen, Ministerie van Veiligheid en Justitie, SSC-I, Rapport Windows 10 – Verkeersstromen en Diagnostic Data, Departementaal Vertrouwelijk, 11 februari 2019.
[13] Bundesambt für Sicherheit in der Informationstechnik, Work Package 4: Telemetry, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-

Dialogue with Microsoft

SLM Rijk has an ongoing dialogue with Microsoft and has informed Microsoft in an early stage about this new Windows 10 DPIA. On 1 February 2019, Microsoft has provided documents from its Supplier Security & Privacy Assurance program, specifically the Microsoft Supplier Data Protection Requirements that are part of the Master Supplier Services Agreement (MSSA).

SLM Rijk has asked Microsoft to give its view on the facts this DPIA is based on, as described in the findings in part A of his DPIA. SLM Rijk has sent part A to Microsoft by mail of 25 February 2019. Though Microsoft initially agreed to provide written input, and a representative of Microsoft Netherlands was present during the presentation of the results for government CIOs and CISOs on 5 March 2019, on 8 March 2019 Microsoft informed SLM Rijk that it saw no mistakes in part A but refrained from providing input. On 19 March 2019 Microsoft did provide brief written input, pointing to factual errors, and providing references to public sources of information.[14] Microsoft did not provide in line comments. Microsoft has marked its reply as Microsoft confidential. Therefore it cannot be attached to this DPIA report.

Early in May 2019, Microsoft has provided further confidential input to this DPIA report.

With the introduction of Windows 10 Enterprise version 1903, Microsoft has enabled the Windows Update function at the Security level of telemetry. Previously this update functionality was only available at Basic or higher levels of telemetry.[15]

Microsoft has provided the following quotable summary of this improvement:

"*Admins in the Dutch Central Government can deploy Windows 10 Enterprise by setting the diagnostic data level to Security and disabling the Timeline cloud sync feature. This allows for sufficient Windows 10 Enterprise functionality while limiting diagnostic data transfers to a level which SLM Rijk considers acceptable in the interim. Microsoft is releasing an update in May that enables Windows Update for Business functionality when the diagnostic data level is set to Security or higher, which adds significant value in keeping our IT environment up-to-date, secure and performing properly.*"

Last but not least, as a result of the ongoing dialogue with SLM Rijk, Microsoft has announced that it is working on a structural solution for Windows 10 Enterprise customers that would want to use the telemetry level Basic or higher.

Microsoft writes: "*SLM Rijk is providing significant input to an upcoming structural solution for Windows 10 Enterprise customers, which is being designed for Windows*

Sicherheit/SiSyPHus/Workpackage4_Telemetry.html (URL last visited and recorded on 20 March 2019).

[14] Microsoft, Windows Insiders get first look at new privacy screen settings layout coming to Windows 10, 6 March 2018, URL: https://blogs.windows.com/windowsexperience/2018/03/06/windows-insiders-get-first-look-new-privacy-screen-settings-layout-coming-windows-10/#ibJm2xFEg5wZklTV.97 (URL last visited and recorded on 20 March 2019).

[15] Microsoft techcommunity, What's new in Windows Update for Business in windows 10, version 1903, 21 May 2019, URL: https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/What-s-new-in-Windows-Update-for-Business-in-Windows-10-version/ba-p/622064 (URL last visited and recorded on 5 June 2019).

10 Enterprise 1809 and later versions. This will allow the Dutch central government to have a simplified compliance solution for Windows 10 Enterprise at diagnostic data levels above Security. This solution will be ready in the foreseeable future, and Microsoft plans to make an announcement about this structural solution later this year."

Following the remarks from Microsoft, the following factual corrections and clarifications have been added.

1. The report describes that the default setting for telemetry that is presented in the user interface to end users is set to Full. But the information is added that if the IT administrator chooses to suppress the privacy-related set-up experience and does not adjust the setting otherwise (e.g., by group policy), the default diagnostic data level setting is Enhanced.[16] Additionally, the explanation is added that though these privacy unfriendly default settings are problematic in relation to individual users, in case of the Windows 10 Enterprise software administrators only have to switch the setting once on the image they create of a new version.
2. Microsoft confirms that privacy invasive capabilities in the operating system have been turned on by default, such as the camera and the microphone. Microsoft suggests that Windows 10 privacy protections for device capabilities such as camera or microphone are managed at the app level. But this would give an incomplete picture of the data protection risks of the default settings. Therefore the additional explanation is given that Microsoft itself by default grants all in-built Microsoft functionalities and apps access. Only apps that are not included in the OS, that are downloaded via the Microsoft Store must first ask for consent to use these capabilities.
3. The information about Windows Timeline has been corrected. Microsoft confirms that the "Store my activity history on this device" privacy setting is On by default. But the "Send my activity history to Microsoft" privacy setting is Off by default. Microsoft has provided information about two Group Policies for administrators to manage these settings: Publish User Activities[17] and Upload User Activities.[18]

Microsoft also proposes to add more information about the Diagnostic Data Viewer. Microsoft explains that the tool shows data that are queued on the device. If the diagnostic level was changed to a lower level before data was sent to Microsoft, the queued data will continue to be displayed in the Diagnostic Data Viewer although it will not be sent. To prevent any misunderstandings about the quality of the technical tests, an explanation is added to this DPIA that every test session has been performed on a separate VM. Because of the default telemetry setting to 'Full' during first install, it is inevitable that some telemetry data are collected on the device before the admin is able to lower the telemetry level to Security.

[16] Since the autumn 2018 versions, the telemetry level Enhanced no longer exists in the different Windows 10 Enterprise versions, only for Windows 2016 server.
[17] Microsoft, Policy CSP - Privacy, Privacy/PublishUserActivities, 14 August 2018, URL: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-privacy#privacy-publishuseractivities (URL last visited and recorded on 5 June 2019).
[18] Ibid., Privacy/UploadUserActivities, URL: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-privacy#privacy-uploaduseractivities (URL last visited and recorded on 5 June 2019).

Outline

This assessment follows the structure of the Model Gegevensbeschermingseffectbeoordeling Rijksdienst (DPIA) (September 2017).[19] 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 tested Windows 10 set-up in detail. This starts with a description of the technical way the diagnostic 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 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 about Windows 10.

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 Windows 10 software, even after applying measures to mitigate the risks.

This data protection impact assessment was carried out by Privacy Company as commissioned by the Dutch ministry of Justice and Security, between January and May 2019.

[19] The Model Data Protection Impact Assessment federal government (DPIA). For an explanation and examples (in Dutch) see: https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia (URL last visited and recorded on 20 March 2019).

Part A. Description of the Windows diagnostic data processing

This first part of the DPIA provides an overview of established facts about the diagnostic data collection via the Microsoft Windows 10 Enterprise software. This starts with a short description of the different telemetry levels. Paragraph 1.3 provides an explanation why higher telemetry levels are out of scope of this DPIA.

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 controller and as data processor. This section also provides an overview of the different interests related to this processing, and of the retention periods.

1. The processing of diagnostic data by Windows 10 Enterprise

Technically, Microsoft Corporation systematically collects diagnostic data about the individual use of the Windows 10 software (not limited to the Enterprise version). Via the in-built telemetry client, Microsoft automatically collects telemetry data on the device, and regularly sends these to its cloud servers in the USA.

The Windows 10 telemetry data stream sent to the Microsoft servers in the USA is separate from, and independent of, the telemetry data stream generated by Microsoft Office.

The Window 10 software is deployed on a large scale by different governmental organisations in the Netherlands, such as ministries, the judiciary, the police and the taxing authority. Approximately 300.000 government employees work daily with the software, often in combination with Microsoft Office software.

Generally, these organisations procure separate bulk licenses for Windows 10 Enterprise and store the content they produce with the Office software in governmental data centres, *on premise*. The Dutch government currently tests the use of the online SharePoint / OneDrive cloud storage facilities. Therefore, this DPIA also assesses the risks of a hybrid deployment, with data created on the Windows operating system stored in SharePoint Online and OneDrive for Business.

Different telemetry settings
Microsoft offers two telemetry settings to end-users in the different versions of Windows 10 Pro, Basic and Full. In the Windows 10 Enterprise version, the IT-pro's (the *administrators* of the Enterprise version) can choose the additional level of Security.

Scope
The aim of this DPIA is to ensure that the data protection rights of data subjects, in this case, employees of the Dutch government, are protected and respected in relation to their use of Windows 10 software at work. To achieve this goal, this DPIA assesses

what the available privacy options are for the organisations that use the software, and what the risks for the privacy of the employees 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 with the two most limited types of telemetry settings in Windows 10 Enterprise: Security and blocking of endpoints in the Microsoft cloud for telemetry traffic.

Generally, government organisations store the content they produce with the Office software in governmental data centres, *on-premises*. This DPIA also assesses the risks of hybrid deployments, with data stored in SharePoint Online/OneDrive for Business.

Some attention has been paid to two relatively new components of Windows 10 Enterprise: Windows Analytics and Windows Timeline.

Windows Timeline is based on the 'Activity History'. This functionality is switched ON by default and stores data about user activities on the local device of the user, such as the names and locations of files the user has worked on. When employees choose to share their activity history with Microsoft, to be able to continue with their work on another device, Microsoft collects and shows the history of visited URL's with Internet Explorer, Edge and Chrome. If those employees work in a hybrid environment, Microsoft also collects the names of accessed (Word) files and storage locations of documents in SharePoint Online. Timeline has been introduced in the Windows 10 April 2018 Update, also known as Redstone 4.

Additionally, the storage of and access to documents in the cloud storage services of Microsoft SharePoint Online and OneDrive for Business are in scope of this DPIA, to get a more realistic view of the risks for data subjects.

The different technical deployments are described in more detail in section 8 of this report, *Techniques and methods of data processing*.

Out of scope
This DPIA does not describe the specific deployments chosen by the different government organisations that procure the Windows 10 Enterprise software (see section 8 in the DPIA). This DPIA can only provide a general overview of the risks and different available privacy settings and options for the different organisations and the end users. It is up to the different organisations 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.

Obviously, this DPIA does not describe the telemetry data collected in the consumer and Pro versions of Windows 10.

The Basic and Full levels of telemetry are also out of scope. The risks of data processing at these levels are out of scope, because it follows from Microsoft's public documentation that at these levels, Microsoft can collect confidential or sensitive personal data.

This report assumes that all government organisations follow the recommendation from the previous Windows 10 DPIA to set the level of telemetry to the Security level. At this minimum level, Microsoft does not capture events about the content from the

different Office applications and the browser Edge. The use of the Advertising ID is therefore also out of scope, because this ID is not collected at the Security and Basic level of telemetry.[20]

The new service Windows Analytics provides information to organisations about the efficiency and health of Windows devices in their environment, based on the collected telemetry data. This service requires Basic or higher level of telemetry and is therefore out of scope of this report.[21]

Data collection at Basic and Full telemetry levels
Microsoft describes several events that may collect sensitive personal data from the contents of Office applications if the Windows telemetry level is set to Basic or Full.

At the Basic level, according to Microsoft's own documentation about the contents of the telemetry events, the company collects information about all installed apps and add-ins (name, publisher, version, locale, and for apps the frequency of use per boot session and the user ID known by the application), via the events Common Data Extensions.app, Microsoft.Windows.Inventory.Core.InventoryApplicationAdd and Microsoft.Windows.Inventory.General.InventoryMiscellaneousOfficeAddInAdd.[22]

Information about the installed apps and add-ins can be used to infer sensitive categories of information, for example if the apps or add-ins are designed to aid people with disabilities.[23]

At the Full level, Microsoft can collect crash dump types about different applications, except for heap dumps and full dumps.[24] Such dumps may reveal personal data about the behaviour of individual users. At the Full level, Microsoft can also collect user content, if a device experiences problem that are difficult to identify or repeat using Microsoft's internal testing. Microsoft explains: "*This data can include any user content that might have triggered the problem and is gathered from a small sample of devices that have both opted into the **Full** diagnostic data level and have exhibited the problem*."

Even though the telemetry streams generated by Windows and by Office are separate, and independent from each other, at the full level of telemetry, the Windows 10 telemetry can also capture rich events about the use of the different Office

[20] At the Basic level, Microsoft explains in its information about the contents of telemetry events that it only collects information whether the Advertising ID is collected or not.
[21] Microsoft techcommunity, What's new in Windows Update for Business in Windows 10, version 1903. "*Please note; however, that Microsoft analytics tools such as Windows Analytics still require a higher diagnostic data level in order to surface deployment insights.*"
[22] Microsoft, Windows IT Pro Center, Windows 10, version 1809 basic level Windows diagnostic events and fields, last updated 19 April 2019, URL https://docs.microsoft.com/en-us/windows/privacy/basic-level-windows-diagnostic-events-and-fields-1809 (URL last visited and recorded on 5 June 2019).
[23] Microsoft, Office Accessibility Center - Resources for people with disabilities, URL: https://support.office.com/en-us/article/Office-Accessibility-Center-Resources-for-people-with-disabilities-ecab0fcf-d143-4fe8-a2ff-6cd596bddc6d (URL last visited and recorded on 5 June 2019).
[24] Microsoft, Windows IT Pro Center, Configure Windows diagnostic data in your organization, 4 April 2018.

applications, such as Outlook, Word, PowerPoint and Excel. This would pose an additional risk for the employees.

At the Full telemetry level Microsoft may collect data from the contents of files for spelling and translation services. Microsoft explains: *"At diagnostic data levels **Enhanced** and **Full**, Microsoft uses Linguistic Data Collection info to improve language model features such as autocomplete, spellcheck, suggestions, input pattern recognition, and dictionary."* Microsoft acknowledges: *"Linguistic Data could contain sensitive information, such as credit card numbers, usernames and passwords, email addresses, or other similarly sensitive information for Linguistic Data Collection. We guard against such events by using technologies to identify and remove sensitive information before linguistic data is sent from the user's device. If we determine that sensitive information has been inadvertently received, we delete the information."*[25]

Regardless of organisational and technical measures introduced by Microsoft to delete data after the collection, the processing of sensitive personal data collected through inking and typing by Microsoft is unlikely to comply with governmental privacy and confidentiality requirements.

Out of scope of this DPIA as well is the collection of telemetry data by customers themselves, via the System Centre (which is based on Windows Analytics). The default setting in Windows 10 Enterprise for System Centre diagnostic data gathering is 'On'. However, setting the operating system diagnostic data level to Basic (or Security) will turn off System Centre diagnostic data, even if the System Centre diagnostic data switch is turned on.[26]

Given the limited time to conduct this DPIA, other choices had to be made about the scope. This DPIA does not address data protection risks caused by remote log-in through a Windows client on a Windows 2016 server. In that case, Microsoft may collect telemetry in two different ways. This DPIA also does not address possible data protection risks resulting from the use of Mobile Device Management in the Microsoft Azure environment. Finally, this DPIA also does not assess the risks of the combination of Windows 10 diagnostic data with LinkedIn diagnostic data.

1.1 Technical analysis of data

This report is based on the thorough analysis of the contents of the telemetry data as collected by the test lab created by SSC-I. In close dialogue with Privacy Company, the technical lab has performed four minutely documented scenario's on virtual machines and Surface pro 3 running Windows 10 Enterprise software version 1809 and either Microsoft Office Professional Plus 2016 MST – Monthly Channel, 1811 (build 11029.20108 Click to run), or Microsoft Office 365, Subscription Microsoft Office 365 ProPlus – Semi Annual Channel, version 1803 (Build 9126.2336 Click to run).

The scenarios were written to represent actual common use of the Windows 10 software by government employees. As recommended by Microsoft the scenarios were kept short and simple, to be able to link recorded telemetry events back to specific activities. The tests were run for a period of 3 days each.

[25] Ibid. Microsoft explains the organisational measure that Microsoft's privacy governance team, including privacy and other subject matter experts, must approve a diagnostics request made by a Microsoft engineer at the Full level before the engineer can start to collect the specific content data.

[26] Ibid., header 'Enterprise management'.

4 tested scenario's diagnostic data Windows 10 Enterprise

1. Desktop, On Premise AD, Telemetry Security (Analytics On[27])
2. Desktop, On Premise AD, Telemetry disabled (Analytics Off)
3. Desktop, Hybrid AD, Telemetry Security (Analytics On)
4. Desktop, Hybrid AD, Telemetry Disabled (Analytics Off)

In the scenario with a Hybrid AD, a VM with Windows 10 Enterprise client was connected to an on-premise Active Directory domain, and the identities were synced with the Office 365 accounts, based on the Office 365 E5 license structure.

Windows 10 comes with pre-installed apps such as Internet Explorer, Edge, Notepad, On-screen keyboard, Magnifier, Microsoft News, Windows Maps, Windows Mail, Weather, File Explorer, Search, OneNote 2016. All these apps have been used in the tested scenarios.

In order to best reflect the reality of Windows 10 usage by government institutions, in every scenario, the following additional software, apps and documents were installed on the VM:

1. Fiddler
2. Chrome browser
3. Adobe reader
4. Citrix Workspace app
5. Microsoft Diagnostic Data Viewer
6. Microsoft Office
   a. Onprem – Office2016
   b. Hybrid – Office365
7. Word document in "Mijn documenten"
   a. "Bijlage 1 Arbodossier Maartje Simmons.docx"
   b. "Bijlage 2 CV Maartje Simmons.docx"
8. Microsoft Outlook with inbox and some test e-mails

The technical lab relied on the (separately installed) Diagnostic Data Viewer as a means to inspect the outgoing telemetry. As an essential security measure, Microsoft encrypts the outgoing traffic to its own servers in a way that makes inspection of the content of the traffic impossible with normal proxy-techniques.[28] The technical lab recorded all outgoing network traffic with Fiddler. This setup ensured that any unexpected network traffic would be noticed. The lab has exported the collected telemetry data in a .csv file and has created an archive with the used virtual machine images.

[27] Microsoft notes in its view on this report from 19 March 2019 that this scenario is invalid, because Analytics requires at least the Basic level of telemetry. The lab research has verified this statement by testing the use of Windows Analytics at the Security level. These tests confirm that Windows Analytics remain empty if the Security level is selected. Analytics has subsequently been removed from the scope of this report.

[28] Microsoft explains: *"All diagnostic data is encrypted using SSL and uses certificate pinning during transfer from the device to the Microsoft Data Management Service."* Microsoft, Windows IT Pro Center, Configure Windows diagnostic data in your organization, 4 April 2018.

Some apps detected the network interception by Fiddler and stopped functioning. This was the case for the Citrix Workspace app, Microsoft News, Windows Maps, Windows Mail and Weather app. Therefore, with the methodology used for this test, not all data flows could be detected.

The lab tests show that disabling telemetry via the registry key or a group policy is not enough to prevent all network traffic. While telemetry is disabled, there is still outgoing traffic to in-built end points in the Microsoft cloud.[29] To prevent the additional risks of leaking personal data to Microsoft, in addition to the level of disabled telemetry, all traffic to these known telemetry end points has been blocked.

The main findings with regard to the two tested telemetry levels are the following:

- Use of the internet browsers results in a large increase of the traffic data. Most of the traffic is functional, to show the requested information about the visited websites
- Microsoft Office ProPlus has its own telemetry end points that are not influenced by the Windows 10 telemetry functionality
- Use of the Citrix client does not result in extra telemetry traffic
- Use of the in-built functionalities in the Windows 10 OS also does not generate extra telemetry traffic
- It was not possible to capture potential traffic through the extra Microsoft apps with Fiddler. The Microsoft apps are programmed to build a secure tunnel to Microsoft. They stopped functioning as soon as Fiddler was switched on.
- If a user has enabled synching of activities in the Microsoft Cloud via Microsoft Timeline, Microsoft registers which internet sites have been visited, and what files have been opened. In the test, traffic from both Microsoft browsers was shown in Timeline, but not from Chrome. At the time, Timeline only recorded activities in Microsoft's two own browsers. Microsoft has meanwhile released an extension to include Chrome traffic.[30] In the hybrid set-up Timeline records the names and locations of files (folder names) in SharePoint Online. Timeline does not show files on the local network.

In GDPR terms SLM Rijk acts as a representative for the government organisations that use the Windows 10 software. This umbrella DPIA report can assist the *administrators* to select a privacy-compliant deployment and conduct their own DPIA's where necessary.

In the current Enrolment framework with underlying documents signed between Microsoft and SLM Rijk, the use of telemetry data with regard to Timeline is not specifically mentioned. This will be explained in more detail in section 4 of this report '*Purposes*'.

Generally, Microsoft considers itself to be the data controller for Windows 10 services, including the telemetry data, except for Windows Analytics and ATP. This will be explained in more detailed in section 5 of this report '*Data controller or data processor*'

[29] The contents of these encoded data have not been examined and were not shown in the Diagnostic Data Viewer.

[30] Windows Central, Microsoft releases official Windows 10 Timeline extension for Google Chrome, 19 February 2019, URL: https://www.windowscentral.com/microsoft-releases-official-windows-10-timeline-extension-google-chrome (URL last visited and recorded on 5 June 2019).

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. To help readers understand the data protection risks, this section explains in detail why the stored diagnostic data about the use of the Windows 10 software are personal data as defined in article 4(1) of the General Data Protection Regulation (GDPR).

This umbrella DPIA can only indicate types of personal data and types of data subjects that may be involved in the processing via the diagnostic data, but it cannot assess the specific risks of the factual data processing per organisation that uses the Windows 10 software. The risks strongly depend on their privacy choices and settings, and the nature of the work performed by their employees. Paragraph 1.3 provides examples of sensitive and confidential personal data Microsoft may process if an organisation does not follow the advice to select the Security level of telemetry. However, these data are out of scope of this DPIA.

Below, the diagnostic data that Microsoft collects via the Security telemetry level are shown in a table. The different kinds of data that Microsoft processes via the Windows 10 diagnostic dataflow, will be described in more detail in section 3 of this DPIA, *Processing of diagnostic data via Windows 10 Enterprise*.

2.1 Data viewer tool

Following the investigation by the Dutch DPA into the Windows 10 telemetry data in 2017[31], Microsoft offers a Diagnostic Data Viewer in all Windows 10 versions issued globally since the spring of 2018. This tool allows end-users and administrators to inspect the telemetry data that are collected on the device. In response to the facts stated in Part A of this DPIA, Microsoft has explained that the tool shows data that are queued on the device. If the diagnostic level was changed to a lower level before data were sent to Microsoft, the queued data would continue to be displayed in the Diagnostic Data Viewer although they would not be sent.[32]

To prevent any misunderstandings about the quality of the technical tests, the technical lab has performed every test session on a separate VM. This excludes possible contagion from collection of data at different telemetry levels. Because of the default telemetry setting to 'Full' during first install, it is inevitable that some

[31] See the Press release of the Dutch DPA 13 October 2017, Microsoft breaches data protection law with Windows 10, URL: https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-microsoft-breaches-data-protection-law-windows-10. A summary in English of these findings is available at the URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/public_version_dutch_dpa_informal_translation_summary_of_investigation_report.pdf. The original report of findings, in Dutch only: AP, Rapport definitieve bevindingen Microsoft Windows 10, De verwerking van persoonsgegevens via Telemetrie -met correcties 6 oktober 2017-, URL: https://autoriteitpersoonsgegevens.nl/ sites/default/files/01_onderzoek_microsoft_windows_10_okt_2017.pdf.

[32] Microsoft written view on Part A of this DPIA, 19 March 2019.

telemetry data are collected on the device before the admin is able to lower the telemetry level to Security.

A typical Windows telemetry event contains a unique number, a timestamp, several unique identifiers for the end-user and the device, and different bits of information about for example the type of device, screen size, operating system, software and/or driver. These data can also form a unique identifier of a user when combined with other over time. Paragraph 8 of this DPIA report, 'Techniques and methods of the data processing' will elaborate on the fact that all diagnostic data are stored in a short term and in a long-term database, thus providing Microsoft with many identifiers relating to a single user over time.
Information in the telemetry events that starts with 'data', contains information about the contents of a specific activity or type of information in a specific telemetry event. All fields that do not start with 'data' contain generic telemetry information that is common for all telemetry events.

The definition of personal data in the GDPR specifically includes online identifiers.

During this assessment, Microsoft was not found to collect sensitive personal data about the use of Windows 10, nor content from files processed through Windows 10 nor otherwise remarkable data because of their confidential nature via the Windows 10 telemetry data stream.

2.2 Data observed at the Security level

At the Security level, Microsoft only collects 4 identifiers and limited types of information. Microsoft collects data about three types of events.

- Information to **configure the in-built telemetry software** (The Connected User Experiences and Telemetry component). The data gathered by the client for this request includes OS information, device id (used to identify what specific device is requesting settings) and device class (for example, whether the device is server or desktop).
- **Malicious Software Removal Tool (MSRT)** The MSRT infection report contains information, including device info and IP address.
- **Windows Defender/Endpoint Protection**. These events collect anti-malware signatures, diagnostic information, User Account Control settings, Unified Extensible Firmware Interface (UEFI) settings, and IP address.[33]

Microsoft writes: "*The Security level gathers only the diagnostic data info that is required to keep Windows devices, Windows Server, and guests protected with the latest security updates. (…) no Windows Update information is gathered at this level, important information about update failures is not sent.*"[34] At the Security level Microsoft promises not to collect user content, such as user files or communications, and also, to prevent collecting direct identifiers. "*We take steps to avoid gathering any information that directly identifies a company or user, such as name, email address, or account ID*."[35]

[33] Microsoft, Windows IT Pro Center,, Configure Windows diagnostic data in your organization 4 April 2018.
[34] Ibid.
[35] Ibid.

The data collected at the Security level (in the Hybrid set-up)[36] are described in the table below, with the public explanations provided by Microsoft. During the test set-up no changes were made to the Security level. That is, both the MSRT and the Windows Defender/Endpoint Protection were left On, and not turned off, in order to get a complete view of the telemetry data at the Security level.

Table 1: identifiers in telemetry events at security level

Identifier	Collected by Event names	Microsoft explanation
Device LocalId	All	A locally-defined unique ID for the device. This is not the human-readable device name. Most likely equal to the value stored at HKLM\Software\Microsoft\SQMClient\MachineId
User LocalId	All	Represents a unique user identity that is created locally and added by the client. This is not the user's account ID.
cdnIp[37]	Microsoft.OSG.DU.DeliveryOptClient.DownloadCompleted	The IP address of the source CDN.
WUDeviceID	SoftwareUpdateClientTelemetry.CheckForUpdates SoftwareUpdateClientTelemetry.UpdateDetected SoftwareUpdateClientTelemetry.Download SoftwareUpdateClientTelemetry.Install	The unique identifier of a specific device, used to identify how many devices are encountering success or a particular issue.

The full list of the observed telemetry event types at the Security level is:

- DxgKrnlTelemetry.GPUAdapterInventoryV2
- Microsoft.OSG.DU.DeliveryOptClient.DownloadCompleted
- Microsoft.OSG.DU.DeliveryOptClient.DownloadStarted
- Microsoft.Windows.StoreAgent.Telemetry.CompleteInstallOperationRequest
- Microsoft.Windows.StoreAgent.Telemetry.EndAcquireLicense
- Microsoft.Windows.StoreAgent.Telemetry.EndDownload
- Microsoft.Windows.StoreAgent.Telemetry.EndInstall
- Microsoft.Windows.StoreAgent.Telemetry.EndScanForUpdates
- Microsoft.Windows.StoreAgent.Telemetry.EndSearchUpdatePackages
- Microsoft.Windows.StoreAgent.Telemetry.EndStageUserData
- Microsoft.Windows.StoreAgent.Telemetry.FulfillmentComplete
- Microsoft.Windows.StoreAgent.Telemetry.FulfillmentInitiate
- Microsoft.Windows.StoreAgent.Telemetry.InstallOperationRequest
- Microsoft.Windows.StoreAgent.Telemetry.SearchForUpdateOperationRequest
- SoftwareUpdateClientTelemetry.CheckForUpdates

[36] At first instance, the lab did not see any telemetry messages in the Data Viewer Tool at the Security level. Close analysis of all captured data shows which data are nonetheless captured.
[37] This is probably the IP address of a proxy, not related to the system or the user.

- SoftwareUpdateClientTelemetry.Download
- SoftwareUpdateClientTelemetry.Install
- SoftwareUpdateClientTelemetry.UpdateDetected
- TelClientSynthetic.HeartBeat_5

These events do not seem to match with the three specific categories of events described by Microsoft (configuration of the CUET, MSRT and Windows Defender information).

For example, the event DxgKrnlTelemetry.GPUAdapterInventoryV2 provides information about the graphic processor and does not seem necessary to configure the telemetry component. Microsoft describes the purpose of this category of events as: "*this event sends basic GPU and display driver information to keep Windows and display drivers up-to-date.*"[38]

Since all telemetry events contain a field with a very detailed timestamp (for example: "2019-01-23T07:12:47.3865298Z"), and the unique identifiers in the user and device localid, Microsoft is technically capable to combine multiple events about a single user, and thus *single out* a user.

End-users in the Microsoft Enterprise environment have a domain account. But if they want to use the Online Services, such as OneDrive, SharePoint Online, Skype, the Microsoft Store or Timeline (when Timeline is used in the hybrid set-up to sync with SharePoint Online), they must also have a Microsoft account. End-users are able to use their work email address to sign up for a Microsoft account. The service turns the requesting user's email address into a Microsoft account.

It is not clear in what circumstances Microsoft creates a shadow Live account if an end-user has only created a local account, on a stand-alone device. This behaviour was observed in the Office ProPlus DPIA, in the results of the audit log.[39]

During this assessment, **at the Security level (and telemetry blocked) no user content (from e-mails or files) was observed in the Windows 10 diagnostic dataflow, nor were any file names or file paths recorded when documents were accessed from SharePoint Online.** However, outside of the telemetry client, when users are not prevented from synching their activity history in the Microsoft cloud and the Timeline functionality is used in a hybrid deployment, Microsoft does collect the names of accessed (Word) files and storage locations of documents in SharePoint Online. With the cloud synced Timeline, Microsoft also collects and shows the history of visited URL's with Internet Explorer, Edge and (since February 2019)

---

[38] Microsoft, Windows IT Pro Center, Windows 10 version 1809 basic level Windows diagnostic events and fields, last updated 19 April 2019, URL https://docs.microsoft.com/en-us/windows/privacy/basic-level-windows-diagnostic-events-and-fields-1809#dxgkerneltelemetry-events (URL last visited and recorded on 5 June 2019). The same information is available for version 1903, 23 April 2019, URL: https://docs.microsoft.com/en-us/windows/privacy/basic-level-windows-diagnostic-events-and-fields-1903#dxgkerneltelemetry-events (URL last visited and recorded on 5 June 2019).

[39] See footnote 132 in the Office ProPlus DPIA report: "*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.*" Microsoft has not provided information about this creation of shadow accounts.

Chrome.[40] Information about visited URL's is considered highly sensitive, as it may reveal special categories of data.

2.3 Results of detailed German telemetry inspection

The German Federal Office for Information Security (Bundesambt für Sicherheit in der Informationstechnik) has conducted a thorough analysis of the technical components built into Windows 10 that log events and create telemetry data. The analysis addresses all the different consumer, professional and Enterprise versions of Windows 10. The different reports with the results were published on 20 November 2018.[41]

Though BSI concludes that Microsoft is able to collect a lot of information through telemetry about the system and the individual usage of the software, the published reports do not provide any details about the type and content of telemetry events. The BSI reports contain a detailed description of the inner workings of the Windows components responsible for the local processing and transmission of the telemetry data.

The BSI did not use the new Data Viewer Tool that is provided by Microsoft to inspect the telemetry data, but instead, used a debugger tool to capture telemetry data while they are being processed by the internal Windows components, before they are encrypted and transmitted to Microsoft.

Microsoft has encrypted the network traffic and has implemented *certificate pinning* as a regular security measure against unauthorised access. However, the specific way in which Microsoft has implemented the certificate pinning, also prevents a trusted network proxy from inspecting the data, i.e., the use of a *man in the middle proxy*. That is why BSI used the debugger tool. The use of this method results in a view of the telemetry data that is similar to the Diagnostic Data Viewer provided by Microsoft.

The BSI report gives an in-depth technical explanation of the functionality of telemetry. The report explains that Microsoft uses 'Event tracing for Windows' (ETW) to collect the telemetry data. ETW is the core logging mechanism of the Windows operating system. It is designed to collect system crash and usage data. The ETW sessions deliver data to the in-built telemetry client for storage on the device, and later, bundled, transfer to Microsoft.

---

[40] The Chrome functionality for Timeline was added by Microsoft on 19 February 2019, after the technical inspection by the test lab at SSC-I. See for example Digital Trends, Microsoft extension adds Google Chrome support for Windows Timeline, 26 February 2019, URL: https://www.digitaltrends.com/computing/google-chrome-windows-10-timeline/ (URL last visited and recorded on 20 March 2019).

[41] Bundesambt für Sicherheit in der Informationstechnik, Work Package 4: Telemetry, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage4_Telemetry.html (URL last visited and recorded on 20 March 2019). The technical results are available at: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/SiSyPHuS_node.html and https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4_node.html (URLs last visited and recorded on 20 March 2019). A summary in German was published in the e-zine Heise, BSI untersucht Sicherheit von Windows 10, 20 November 2018, URL: https://heise.de/-4227139 (URL last visited and recorded on 20 March 2019).

The events created by ETW are produced by so called ETW providers, the entities that are able to log the telemetry data. Each ETW provider is used for logging a specific category of events. For example, the Transmission Control Protocol (TCP) / Internet Protocol(IP) driver implements its own provider logging network events. In the public documentation of Microsoft, telemetry events are grouped by such providers. This report calls these providers 'categories' of telemetry data, as opposed to individual events within a category, and the different fields with information in each telemetry event.

The number of ETW providers differs enormously per telemetry level, and is also dependent of the actual system usage, installed software and enterprise configuration.[42]

Table 2: number of ETW providers per telemetry level

Telemetry level	**ETW providers[43]**
Security	4
Basic	410
Enhanced	418
Full	422

The BSI finds the options for users and admins to determine the different telemetry levels insufficient, because the data stream is very dynamic. BSI writes that Microsoft is retrieving and updating the configuration telemetry data several times per hour.[44] BSI also warns that setting the telemetry level to the lowest level of Security, does not end the data flow.

Although BSI did not publish an analysis of the contents of the captured telemetry events, the observed behaviour of the telemetry matches with the observations made by the lab with the Data Viewer Tool. Therefore, there are no indications that the Data Viewer Tool would give incomplete access to all telemetry events.

2.4 Timeline data

Both with telemetry set to Security, and with telemetry blocked, Microsoft collects document names and storage location on SharePoint Online when the Timeline cloud sync functionality is turned On. Microsoft similarly processes URLs visited with Microsoft browsers or Google Chrome. Timeline does not reveal document names on the local network to which the device is connected.

2.5 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*

[42] BSI Workpackage 4, full file, Executive Summary, p. 10.

[43] BSI, Work Package 4: Telemetry. Table copied and translated from German to English.

[44] Ibid. The report contains two figures that illustrate the frequency of the communication of DiagTrack with Microsoft's back-end infrastructure. Over a 3 hour interval, every 20 to 25 minutes a connection was established. See p. 31-32.

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 the telemetry data Microsoft collects through the use of Windows 10 are all personal data. During this investigation Microsoft claimed that most Windows 10 telemetry data did not relate to natural persons, but only to (technical aspects of) the operating system. The Dutch DPA explained that when object data are combined with other data, the resulting data set may contain information relating to an individual.

Even at the Security level of Windows 10 telemetry, though Microsoft collects very few data, the collected telemetry data contain several unique identifiers. These identifiers allow Microsoft to combine events about a single user over time. Since all telemetry events also contain a time stamp, Microsoft is technically capable to combine multiple events about a single user, and thus *single out* a user (as described in recital 26 of the GDPR). A Microsoft account is necessary to download apps from the Windows Store, to use OneDrive or (if not prohibited by the administrator) to use the Timeline functionality to sync work activities on multiple devices. End-users generally use their work email address as Microsoft accounts.

Microsoft has the technical means to relate device ID's to a user account, and many Microsoft accounts contain directly identifiable information, because they are based on the work email addresses that generally contain the initials and last name of the employee, as well as the (domain)name of the employer.

Microsoft is able to directly or indirectly identify an individual user. 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 data involves structural data processing. At the highest telemetry level, this may involve up to 1.200 different types of events. Microsoft has explained 10 engineering teams can add events to the data stream. Data events at the different telemetry levels may include (user or device) names and IP-addresses. Such data are either immediately replaced by asterixis in the original event on the device or stored in a hashed form. All telemetry data, both from Windows 10 and from Microsoft Office are long-term stored in the central Cosmos database in the USA. This database may contain logs with unique user identifiers such as User GUIDs, PUIDs, or SIDs (abbreviated by Microsoft as EUPI). These identifiers are pseudonyms.

Microsoft accepts that the diagnostic data may contain personal data, but Microsoft does not consider all diagnostic data to be personal data. Microsoft does not provide documentation which Windows 10 diagnostic data 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.[45]

During the dialogue with Microsoft about the Office telemetry data, Microsoft has stated to SLM Rijk: "*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*

[45] Meeting report SLM Rijk and Microsoft of 28 August 2018, answer to Q2.

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."[46]

To be clear, Microsoft has emphasized that it does not try to identify or track the behaviour of a single user over time. However, the possibility of establishing such a link is enough for the classification of information as personal data. It is not necessary that this process of combining events leading to identification is actually carried out. Similarly, Microsoft is technically capable of combining Windows 10 telemetry data with Office ProPlus telemetry data. The possibilities for Microsoft to process these data for new types of machine learning and artificial intelligence are described in section 8 of this report.

A Microsoft account is necessary to download apps from the Windows Store (including additional Office add-ons, to use OneDrive or (if not prohibited by the admins) to use the Timeline functionality in a hybrid set-up, if SharePoint Online is used. In those cases, Microsoft has the technical means to relate device ID's to a user account, and thus directly identify the individual user. But Microsoft can also indirectly identify users, with the help of the employer, for example through the license number or domain account. The combination of several unique identifiers in the Security level events, with a timestamp and sequence number combined with a storage period of minimum of 30 days, makes it reasonably likely that Microsoft can frequently relate the device ID's to a domain account, by combining of several events over time. For a specialised software company with approx. 300.000 employees, this cannot be considered an unreasonable effort.
Therefore, Microsoft must be held capable of directly or indirectly identifying the individual end-user. Therefore, the collected telemetry data are personal data as defined in Article 4(1) of the GDPR. The collected personal data may present a high risk for employees if they are used to analyse work patterns and monitor employee behaviour, either by Microsoft or by the employer.

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.

As described in section 2.1 of this report, during this assessment, no user content (from files or mails) was observed in the Windows 10 telemetry data stream at the Security (or telemetry blocked) level. This does not mean that Microsoft does not collect sensitive or confidential data via the telemetry stream.

First of all, when the administrator has not centrally prohibited the use of the cloud synchronisation functionality of Timeline, in a hybrid deployment Microsoft collects the names of accessed (Word) files and storage locations of documents in SharePoint Online. In that set-up, Microsoft also collects and shows the history of visited URL's with Internet Explorer, Edge and Chrome. Information about visited URL's is considered highly sensitive, as it may reveal special categories of data.

Second, pre-installed apps such as Mail, News, Maps and Weather stopped working when Fiddler was turned 'On'. Thus, the telemetry stream via these apps could not be analysed.

[46] Footnote 26 of the Office ProPlus DPIA report cites: Microsoft confidential response to this DPIA report, 24 September 2018, p. 21. Though the meetings were about Microsoft Office, the Windows telemetry data are long-term stored in the same Cosmos database.

Third, the collection of telemetry data is highly dynamic. Microsoft engineers can add new types of events to the telemetry stream without prior notice to the users, if they follow internal privacy procedures.[47] According to the BSI research quoted in paragraph 2.2 the configuration of the telemetry data flow is modified several times per hour. Each modification can mean that a new ETW provider wants access to data, or an existing ETW provider wants access to other log data.

Microsoft engineers explain the importance of the dynamic nature of creating telemetry events as follows: "*In data-driven environments, such instrumentation is moving towards rule-based approaches, where instrumentation can be added once and then toggled without having to change the code itself. This functionality has enabled data-driven organizations to collect data not just during testing, but long after the product is deployed into retail. As Austindev remarks, "What's really great for us is to be able to real-time turn on and off what log stuff you're collecting at a pretty granular level. And to be able to get the performance back when it is turned off is a big thing for us."*[48]

Microsoft has explained to the Dutch DPA in 2017 that the collection of telemetry data in Windows 10 is controlled by organisational policy rules. There is no reason to assume that such policy rules would not apply to the collection of telemetry data from Windows 10 Enterprise. However, Microsoft does not provide any information about this policy, nor any audit results with regard to compliance with those policy rules. The limitations to these audits are described in section 5 of this report, 'Controller, processor and sub-processors'.

In the Trust Center, Microsoft provides privacy information about Office 365, Azure, Dynamics 365 and Microsoft Professional (support) services, but not about Windows 10. Nonetheless, Microsoft indicates that the company has privacy teams embedded in the different service groups that do granular reviews of the data processing and present their results to the EU Data Protection Officer.

Microsoft writes:
"*Microsoft practices privacy by design and privacy by default in its engineering and business functions. As part of these efforts, Microsoft performs comprehensive privacy reviews on data processing operations that have the potential to cause impacts to the rights and freedoms of data subjects.* ***Privacy teams embedded in the service groups review the design and implementation of services to ensure that***

[47] Microsoft Support, diagnostics feedback and privacy in Windows-10, 10 April 2019: "*Specific data items collected in Windows diagnostics are subject to change to give Microsoft flexibility to collect the data needed for the purposes described. For example, to ensure Microsoft can troubleshoot the latest performance issue impacting users' computing experience or update a Windows 10 device that is new to the market, Microsoft may need to collect data items that were not collected previously.*" URL: https://support.microsoft.com/en-us/help/4468236/diagnostics-feedback-and-privacy-in-windows-10-microsoft-privacy (URL last visited and recorded on 5 June 2019). Microsoft has previously confirmed that the collection of telemetry data in Office365 ProPlus is similarly dynamic. Meeting report 28 August 2018, answer to Q1.

[48] Titus Bank, Robert DeLine, Steven Drucker and Danyel Fisher:The Bones of the System: A Case Study of Logging and Telemetry at Microsoft, ICSE '16 proceedings of the 38th international conference on software engineering companion, 1, (May 2016), URL: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/PID4092213-1.pdf (URL last visited and recorded on 20 March 2019).

***personal data is processed in a respectful manner that accords with international law**, user expectations, and our express commitments. **These privacy reviews tend to be very granular—a particular service may receive dozens or hundreds of reviews.** Microsoft rolls up these granular privacy reviews into Data Protection Impact Assessments (DPIAs) that cover major groupings of processing, which the Microsoft EU Data Protection Officer (DPO) then reviews. The DPO assesses the risks related to the data processing to ensure that sufficient mitigations are in place. If the DPO finds unmitigated risks, he or she recommends changes back to the engineering group. DPIAs will be reviewed and updated as data protection risks change."*[49]

2.6 Possible types of personal data and data subjects

As highlighted earlier in this report, this DPIA cannot provide the required limitative overview of the different kinds of personal data that will be processed by Windows 10 diagnostic data. However, this report recommends that administrators set the telemetry level to Security, and centrally prohibit the cloud syncing functionality of Windows 10 Timeline. If that advice is followed, Microsoft processes very few personal data.

It is up to the individual organisations however to decide about the telemetry level, and other relevant privacy settings during the actual installation. To assess the risks of these settings, they have to make 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 via Windows, especially since most government organisations also use Microsoft Office. The Office products and other apps than can be installed on the Windows 10 operating system can be used for many different purposes by many different organisations.

However, in this report, only the Security level of telemetry is examined, as well as a set-up in which telemetry traffic is blocked. These settings exclude a richer data collection by Microsoft about the contents of Office files (at the Full telemetry level). Based on the lab tests and Microsoft's own documentation, the diagnostic data collection at the Security level does not include user content.

In a hybrid deployment, the use of Windows Timeline can result in the further processing by Microsoft of data about the names of files and storage locations in SharePoint Online, as well as the collection of surfing behaviour via the browsers Edge and Internet Explorer. These kinds of personal data deserve some extra attention.

Classified Information

Dutch government employees will, depending on the capacity in which they work, often process Classified Information. The Dutch government defines 4 classes of Classified Information, ranging from confidential within the ministry to extra secret state secret.[50]

[49] Microsoft Trust center, Data Protection Impact Assessments FAQ, answer to the question 'What are the responsibilities of Microsoft'?, no date provided, URL: https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/gdpr-dpia (URL last visited and recorded on 5 June 2019).

[50] Defined in: Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013)

Classified Information is not a separate category of data in the GDPR or other personal data legislation. But information processed by the government that is qualified as classified information, whether or not it qualifies as personal data, must legally 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 have chosen a hybrid deployment of Windows 10 Enterprise, with the use of SharePoint Online or OneDrive, they have to be aware Microsoft may further process diagnostic data from its cloud servers which may include confidential file names and storage locations. A folder may for example have as name: "State Secret – negotiations with country/company X". If users are not prohibited from switching on the cross-device sync functionality provided by Timeline, organisations must be aware that Microsoft can further process information from and about government employees, including information which employees regularly access, send or receive labelled information on SharePoint Online or OneDrive, and what websites they have visited in the last 90 days. Of course, even if Timeline is switched Off, Microsoft still collects diagnostic data in system-generated log files from its cloud servers about access to files.

Personal data of a sensitive nature
Some 'normal' personal data have to be processed with extra care, due to their sensitive character. Examples of such sensitive data are financial data, communications traffic data and location data. It is likely that many government employees process personal data of a sensitive nature on a daily basis, but Microsoft does not collect such data at the Security level of Windows 10 Enterprise telemetry.

If employees are not centrally prohibited from using the cloud sync functionality of Timeline, Microsoft can process information via diagnostic data about web surfing behaviour. Even if the websites do not allow for the inference of special categories of data, they are personal data of a sensitive nature, since the URL's reveal information about the interests of employees and employees also have a reasonable expectation that their fundamental right to communications secrecy is also respected, within boundaries, on the work floor.

Employees also have a habit of including their own names in document titles, and organisations may work with document structures in which file paths may include confidential information or for example, qualifications or diseases of the natural persons mentioned in the documents in the folder. The further processing of these diagnostic data via the cloud sync Timeline functionality may thus result in additional data protection risks, on top of the risks caused by the use of cloud storage servers.

Special categories of personal data
Special categories of personal data are especially protected by the GDPR. According to article 9 (1) GDPR, personal information falling into special categories of data is any:
"*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data,*

biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

With special categories of data, the principle is one of prohibition: 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.

If organisations allow employees to switch On the cloud sync functionality of Windows Timeline in a hybrid set-up, where users can upload documents to SharePoint Online or OneDrive, Microsoft can further process the name and the path of files on its own cloud servers and collect the URLs of visited websites. These URL's can be used to infer special aspects of an individual employee, such as religious or political orientation or health data.

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. With the Windows 10 diagnostic data processing set to Security, the risks are limited to employees and other data subjects.

Employees
The government users of the Windows software are employees, contractors and (temporary) workers of a governmental organisation.
Their (account and device) names are processed in connection with the use of the Windows 10 software.

Contact persons
At the basic and security level of telemetry, Windows 10 Enterprise does **not** capture data about contact persons, such as for example in e-mail addresses.

Dutch citizens and other data subjects
Besides employees there is a miscellaneous group of individuals whose personal data may be processed in titles of documents stored in SharePoint Online or OneDrive, for example in the name of a picture or job application.

3. Processing of diagnostic data via Windows 10 Enterprise

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 Windows 10 Enterprise software. 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:

1. Content data
2. Diagnostic data and
3. Functional data

A specific subset of user content data is qualified by Microsoft as 'Customer Data'. This category concerns content data that customers have consciously uploaded via

Online Services such as Azure, Dynamics and Microsoft Office 365 ProPlus to Microsoft datacentres. Microsoft promises, via its Online Service Terms and the specific GDPR amendment negotiated by SLM Rijk, to not use these Customer Data for direct marketing or similar commercial purposes. Users can also determine that Customer Data at rest are only stored in the EU.

Diagnostic data (or telemetry data) are all data about the individual use of the Windows 10 software, including information about the use of Microsoft Office software and other software and apps, but only to the extent that they are stored by Microsoft and not merely transported. Technically, Microsoft collects diagnostic data about and from Windows 10 through an in-built telemetry client. This client collects events on the device, and regularly sends these to the Microsoft servers in the USA. This collection technique 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.

Some data which are generated by the use of the services are functional data, data that necessarily 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 location data processed by a map to provide directions, 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 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.

Microsoft performs the following data processing activities with the diagnostic data:

- Collection of the telemetry data on the device
- Sometimes immediate replacement of strings with letters or numbers by asterixis (as visible in the Data Viewer Tool)
- Sending of the collected telemetry data in a batch over the public internet to its own cloud servers in the USA
- Hashing, scrubbing (partial deletion), masking, pseudonymising or anonymising of the collected data
- Storage of the telemetry data for different periods in a central database in the USA
- Deletion of data.

Microsoft does not provide a public explanation why it is necessary to transmit all telemetry data to servers in the USA, why not store these in the EU, or at least, anonymise the data collected in the EU before they are transferred to the USA.

3.1 Opt-out choice for telemetry

In Article 25 the GDPR obliges data controllers to comply with principles of privacy by design and privacy by default.

Article 25(2) explains: "*The controller shall implement appropriate technical and organisational measures for ensuring that, **by default**, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall*

ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

The qualification of Microsoft as a (joint) data controller is discussed in section 5 of this DPIA report. But regardless of the legal qualification, the GDPR explicitly calls on software manufacturers to implement the privacy by design and by default principles. Recital 78 states: "*When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task,* ***producers of the products, services and applications should be encouraged to take into account the right to data protection*** *when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.*"

The IT-pro's (*administrators*) of the Enterprise version can choose between three telemetry options (Security, Basic or Full). If the administrator chooses to suppress the privacy-related set-up experience and does not adjust the setting otherwise (e.g., by group policy), the default diagnostic data level setting is **Enhanced**.[51] At that level, Microsoft explains it collects "*Additional insights, including: how Windows, Windows Server, System Center, and apps are used, how they perform, advanced reliability data, and data from both the* ***Basic*** *and the* ***Security*** *levels.*"[52]. In that case, the setting for diagnostic data presented to end-users is **set to Full**.

Since Windows 10 version 1809, admins of the government organisations can use a setting to switch the default to the Security level of telemetry. They can disable any individual user choices with regard to the telemetry level.

Admins can also disable telemetry in the Register and block outgoing telemetry traffic to known end points. Microsoft provides documentation about all known telemetry endpoints in the Windows 10 Enterprise 1809 build.[53] Admins can use additional settings, such as disabling ATP and Windows Defender SmartScreen (policy added since version 1809). Admins may also apply the Windows Restricted Traffic Limited Functionality Baseline.[54]

The admin of each government organisation can apply the Security level or block the diagnostic data flow by adjusting settings in the Group Policy or by modifying the Registry. Microsoft explains: "*You can configure diagnostic data at the Security/Basic level, turn off Windows Defender diagnostic data and MSRT reporting, and turn off all*

[51] Added at the request of Microsoft, remark made in its view on the report of 19 March 2019. Microsoft refers to its documentation in the Windows IT Pro Center, Configure Windows diagnostic data in your organization, 4 April 2018. Since the autumn 2018 versions, the telemetry level Enhanced no longer exists in the different Windows 10 Enterprise versions as a choice for users, only for Windows 2016 server.

[52] Ibid.

[53] Microsoft Windows IT Pro Center, Manage connection endpoints for Windows 10, version 1809, 16 May 2019, URL: https://docs.microsoft.com/en-us/windows/privacy/manage-windows-1809-endpoints (URL last visited and recorded on 5 June 2019).

[54] Ibid. The Microsoft Windows Restricted Traffic Limited Functionality Baseline is available for versions 1607 to 1903. Microsoft warns that Windows and Windows Defender have to be updated before applying these settings. URL: https://go.microsoft.com/fwlink/?linkid=828887 [URL last visited and recorded on 5 June 2019]

other connections to Microsoft network endpoints as described in this article to help prevent Windows from sending any data to Microsoft."[55]

Administrators can turn off the Malicious Software Removal Tool (MSRT) using an in-built functionality by Microsoft. The Windows Defender anti-virus functionality can only be disabled permanently with difficulty, through registry keys or group policy settings.

The processing of diagnostic data is partially influenced by the type of network: local, or hybrid. In line with the government PIA model, these different deployments are discussed in more detail in section 8 of this report, *Techniques and methods of the data processing*.

Microsoft describes the settings for the telemetry data in Windows 10 at the different levels as follows[56]

Table 3: Settings and purposes of data collection per telemetry level

Level	Data gathered	Value
Security	Security data only	0
Basic	Security data, and basic system and quality data	1
Enhanced	Security data, basic system and quality data, and enhanced insights and advanced reliability data	2
Full	Security data, basic system and quality data, enhanced insights and advanced reliability data, and full diagnostics data	3

Microsoft explains: "*The lowest diagnostic data setting level supported through management policies is Security. The lowest diagnostic data setting supported through the Settings UI is Basic. The default diagnostic data setting for Windows Server 2016 is Enhanced.*"[57]

3.2 Other privacy choices in Windows 10 Enterprise

Windows 10 contains many components with separate privacy settings. The use of these components can generate extra telemetry data. The privacy choices for Timeline are discussed in a separate paragraph below.

[55] Microsoft Windows IT Pro Center, Manage connections from Windows operating system components to Microsoft services, 16 May 2019.
[56] Since the autumn 2018 versions, the telemetry level Enhanced no longer exists in the different Windows 10 Enterprise versions as a choice for users, only for Windows 2016 server.
[57] Microsoft, Windows IT Pro Center, Configure Windows diagnostic data in your organization, 4 april 2018.

The Advertising ID and Tailored Experiences are turned Off by default, unless the IT Admin takes action to enable them. In practice, the choice is up to the end user. During the set-up (if not disabled by the admin) Microsoft presents a number of privacy choices to the user regarding the telemetry level, location, the use of the Advertising ID, Tailored Experiences, Inking & Typing, Online speech recognition and Find my device.

Aside from these specific privacy choices, Windows 10 contains many services and capabilities that may have a high privacy impact.

Many default settings, as presented in the interface for the end-user, are not privacy friendly. By default, Microsoft switches 'On' the Windows Defender SmartScreen, Website access to the language list, Suggestions for new Content and apps, tracking of app launches, and show 'fun facts, tips, tricks and more' on the lock screen (advertisements). Microsoft also preselects the highest, automatic frequency of providing feedback.[58]
Microsoft also switches 'On' by default privacy invasive capabilities in the operating system, such as location, camera, microphone, the contact list, calendar, notifications, account data, call history, e-mail, planned activities, SMS and mms messages, Bluetooth, access to diagnostic data about other apps, document folders and picture and video libraries. However, in the new 1903 version of Windows 10, launched end of May 2019, Microsoft has added a microphone icon that appears in the notification area alerting users which apps are using the microphone.[59]

In its written view on part A of this report, Microsoft confirms that many capabilities in the operating system have been turned on by default, such as the camera and the microphone. Microsoft suggests to add that Windows 10 privacy protections for device capabilities such as camera or microphone are managed at the app level.[60] But Microsoft itself by default grants all in-built Microsoft functionalities and apps access. Only apps that are not included in the OS, that are downloaded via the Microsoft Store, must first ask for consent to use these capabilities.

It is up to administrators to turn off any privacy unfriendly default settings for data collection through Windows 10 Enterprise. Administrators can determine the settings via Group Policies (*Computer Configuration\Administrative Templates*) or through Mobile Device Management (MDM) settings. If an administrator has chosen to centrally prohibit certain functionalities, the user will see an alert that says '*Some*

[58] Microsoft Support, General privacy settings in Windows 10, 21 May 2019, URL: https://support.microsoft.com/en-us/help/4459081/general-privacy-settings-in-windows-10-microsoft-privacy (URL last visited and recorded on 5 June 2019). See also: The Star, Windows 10 privacy settings: How to stop Microsoft from spying on you, 16 February 2019, URL: https://www.thestar.com.my/tech/tech-news/2019/02/16/windows-10-privacy-settings-how-to-stop-microsoft-from-spying-on-you/ (URL last visited and recorded on 20 March 2019).
[59] Microsoft, What's new for IT pros in Windows 10, version 1903, 21 May 2019, URL: https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/What-s-new-for-IT-pros-in-Windows-10-version-1903/ba-p/622024 (URL last visited and recorded on 5 June 2019). See the specific help tekst at https://support.microsoft.com/en-us/help/4468232/windows-10-camera-microphone-and-privacy (URL last visited and recorded on 5 June 2019).
[60] Microsoft written view on part A of this report, 19 March 2019.

*settings are hidden or managed by your organizatio*n' when they navigate to Start > Settings > Privacy.[61]

3.3 Windows Timeline

Microsoft can collect personal data when the Timeline cloud sync functionality is turned On. This dataflow is separate from the telemetry data.

End-users see an option for 'activity history' in their privacy settings. This option is switched On by default.[62] Microsoft confirms in its view on the facts contained in part A of this DPIA that the "Store my activity history on this device" privacy setting is indeed On by default. But Microsoft also explains that the separate option "Send my activity history to Microsoft" privacy setting is Off by default.[63]
Microsoft explains the functionality of Timeline as follows: "S*ee a timeline of activities and be able to resume those activities from your device. For example, let's say that you were editing a Word document on your device, but you were unable to finish before you had to leave the office for the day. If you selected the Store my activity history on this device check box on the Activity history settings page, you would see that Word activity in your timeline the following day, and for the next several days, and from there, you could resume working on it. If you selected the Send my activity history to Microsoft check box and you were unable to finish before you had to leave the office for the day, not only would you see that Word activity in your timeline for up to 30 days, but you could also resume working on it later from another device."*[64]

The Timeline cloud sync functionality is only available for users with a Microsoft account. This is relevant if government employees work in a hybrid environment, where the local AD is synced with the Office 365 AD. In such a hybrid environment employees can use Microsoft's cloud storage services SharePoint Online and OneDrive for Business.

If users turn the separate cloud sync Timeline option On, they send their activity history to Microsoft. The company then uses data it already has in system-generated log files from its SharePoint online and OneDrive servers to create an online overview of the files the employee has been working on. Microsoft explains: "[Timeline] *uses*

---

[61] Microsoft, Windows IT Pro Center, Windows and the GDPR: Information for IT Administrators and Decision Makers. 11 May 2018, URL: https://docs.microsoft.com/en-us/windows/privacy/gdpr-it-guidance (URL last visited and recorded on 5 June 2019).
[62] PC World, Windows 10 Timeline: How to use Microsoft's new organizational tool, 27 April 2018. "*Windows assumes that you want Timeline turned on. If you don't, or you'd like to manage how Microsoft uses your information, visit the Settings menu at Settings > Privacy > Activity History.*" URL: https://www.pcworld.com/article/3263905/windows/windows-10-how-to-use-timeline.html (URL last visited and recorded on 5 June 2019).
[63] Microsoft names two Group Policies settings for administrators to manage these options: Publish User Activities and Upload User Activities. Microsoft, Policy CSP - Privacy, Privacy/PublishUserActivities, 14 August 2018, URL: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-privacy#privacy-publishuseractivities (URL last visited and recorded on 5 June 2019).and Privacy/UploadUserActivities, URL: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-privacy#privacy-uploaduseractivities (URL last visited and recorded on 5 June 2019).
[64] Microsoft, Windows 10 activity history and your privacy, 10 April 2019, URL: https://support.microsoft.com/en-us/help/4468227/windows-10-activity-history-and-your-privacy-microsoft-privacy (URL last visited and recorded 5 June 2019).

your activity history data to enable cross-device experiences.[65] Microsoft writes: "*You can continue activities that you started from those other devices on your Windows device. Initially, this will be limited to Microsoft Edge mobile, but will soon include Office mobile apps like Word, Excel, and PowerPoint.*"[66]

When the online Timeline functionality is switched On, Microsoft also collects web surfing behaviour by processing information about use of the three browsers Explorer, Edge and Chrome.

4. Purposes of the processing

The Dutch government has a multi-layered enrolment framework with Microsoft to act as data processor for the Enterprise Online Services (such as Azure and Office365) and for Professional Services (such as customer support). But this framework does not include Windows 10 Enterprise, because Microsoft does not consider this to be an Online Service.

4.1 Sixteen processing purposes from the general privacy statement

With regard to the diagnostic data collected by Windows 10 Enterprise, Microsoft considers itself to be a (sole and independent) data controller. Therefore, all the purposes mentioned in Microsoft's general Privacy Statement apply.[67]

Some of the purposes in the General Privacy Statement only apply to specific customer products and services and are therefore not mentioned here.[68]

1. *Purpose: compatible uses with providing the Enterprise 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.*"[69]

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*

[65] Ibid.
[66] Ibid.
[67] Microsoft Privacy Statement, last updated May 2019, URL: https://privacy.microsoft.com/en-GB/privacystatement (URL last visited and recorded on 5 June 2019). Statement under "How We Use Personal Data".
[68] The purposes of Customer Support and Transacting Commerce are excluded, as the first is arranged via Professional Services and it is not possible for employees to carry out a transaction with Microsoft using the Enterprise version.
[69] Microsoft Privacy Statement, May 2019, under Product-specific details: Enterprise and developer products.

Bing search engine, we use that query to display search results to you. Additionally, as communications are a feature of various products, programs and activities, we use data to contact you. For example, we may contact you by phone or email or other means to inform you when a subscription is ending or discuss your licensing account. We also communicate with you to secure our products, for example by letting you know when product updates are available."[70]

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.*"[71]

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***."[72]

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.*"[73]

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.*"[74]

7. *Purpose: Help secure and troubleshoot*

Microsoft processes data in order to secure and troubleshoot its products.
"*We use data to help secure and troubleshoot our products. This includes using data to protect the security and safety of our products and users, detecting malware and malicious activities, troubleshooting performance and compatibility issues to help customers get the most out of their experiences, and notifying customers of updates*

[70] Ibid.
[71] Ibid.
[72] Ibid.
[73] Ibid.
[74] Ibid.

to our products. This may include using automated systems to detect security and safety issues."[75]

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."*[76]

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."*[77]

10. Purpose: Promotional communications

"We use data we collect to deliver promotional communications. You can sign up for email subscriptions and choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail and telephone. For information about managing your contact data, email subscriptions, and promotional communications, see the How to access and control your personal data section of this privacy statement."[78]

11. Purpose: Relevant offers.

"Microsoft uses data to provide you with relevant and valuable information regarding our products. We analyse data from a variety of sources to predict the information that will be most interesting and relevant to you and deliver such information to you in a variety of ways. For example, we may predict your interest in gaming and communicate with you about new games you may like."[79]

12. Purpose: Advertising

"We use data we collect through our interactions with you, through some of our products, and on third-party web properties, for advertising in our products and on third-party properties. We may use automated processes to help make advertising more relevant to you."[80]

13. Purpose: Reporting and Business Operations

Microsoft collects and processes information for reporting and business operations:

[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] Ibid.

"*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.*"[81]

14. 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.*"[82]

15. Purpose: legal compliance

Microsoft notes data subject access obligations under the GDPR as a purpose for data processing:

"*We process data to comply with law. For example, we use the age of our customers to ensure we meet our obligations to protect children's privacy. We also process contact information and credentials to help customers exercise their data protection rights.*" [83]

16. 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.*"[84]

4.2 Four purposes for telemetry at the Security level

Microsoft describes that the purpose for the collection of diagnostic data at the Security level is to provide the customer with the latest security updates.

Microsoft writes: "*The Security level gathers only the diagnostic data info that is required to keep Windows devices, Windows Server, and guests protected with the latest security updates.*" (… This) *includes data about the Connected User Experiences and Telemetry component settings, the Malicious Software Removal Tool, and Windows Defender*."[85]

Microsoft does not provide a limitative overview with a description of the contents and purposes of the different events collected at the Security level.

On the same page, Microsoft provides more specific purposes for the diagnostic data processing at the Security level.

Microsoft writes:

"***Connected User Experiences and Telemetry component settings***

If general diagnostic data has been gathered and is queued, it is sent to Microsoft. Along with this diagnostic data, the Connected User Experiences and Telemetry

[81] Ibid.

[82] Ibid.

[83] Ibid.

[84] Ibid.

[85] Microsoft, Windows IT Pro Center, Configure Windows diagnostic data in your organization, 4 April 2018.

component may download a configuration settings file from Microsoft's servers. This file is used to configure the Connected User Experiences and Telemetry component itself. The data gathered by the client for this request includes ***OS information, device id (used to identify what specific device is requesting settings) and device class*** *(for example, whether the device is server or desktop).*

Malicious Software Removal Tool (MSRT)
The MSRT infection report contains information, including ***device info and IP address****. Microsoft explains in a note that administrators can turn off the MSRT infection report. No MSRT information is included if MSRT is not used.*[86]

Windows Defender/Endpoint Protection*.*
Windows Defender and System Center Endpoint Protection requires some information to function, including ***anti-malware signatures, diagnostic information, User Account Control settings, Unified Extensible Firmware Interface (UEFI) settings, and IP address****."*[87]

Microsoft also explains: "*No user content, such as user files or communications, is gathered at the Security diagnostic data level, and we take steps to avoid gathering any information that directly identifies a company or user, such as name, email address, or account ID. However, in rare circumstances, MSRT information may unintentionally contain personal information. For instance, some malware may create entries in a computer's registry that include information such as a username, causing it to be gathered. MSRT reporting is optional and can be turned off at any time.*"[88]

It follows from this information that Microsoft processes the diagnostic data collected at the Security level for four purposes, namely:

1. Providing the customer with the latest security updates
2. The configuration of the telemetry pipeline
3. Detection and removal of malicious software
4. Windows Defender anti-virus and endpoint security protection

4.3 Four purposes for Timeline

Microsoft describes the following specific purposes for the processing of data via Timeline when users have switched on the cloud sync functionality: "*Microsoft uses the activity history data to provide you with personalized experiences (such as ordering your activities based on duration of use) and relevant suggestions (such as anticipating what your needs might be based on your activity history).*"[89] At the bottom of this information page, Microsoft mentions the following additional purposes: "*Microsoft will also use your activity history to improve Microsoft products and services when the setting for sending your activity history to Microsoft is enabled. We do this by applying machine-learning techniques to better understand how customers in*

[86] Microsoft refers for more information to its guidance in Windows Support for Windows 7 Enterprise, Deploy Windows Malicious Software Removal Tool in an enterprise environment, URL: https://support.microsoft.com/en-us/help/891716/deploy-windows-malicious-software-removal-tool-in-an-enterprise-enviro (URL last visited and recorded 5 June 2019).
[87] Microsoft, Windows IT Pro Center, Configure Windows diagnostic data in your organization, 4 April 2018.
[88] Ibid.
[89] Microsoft, Windows 10 activity history and your privacy, 10 April 2019.

general use our products and services. We also diagnose where customers encounter errors and then help fix them."[90]

Thus, Microsoft processes the Timeline data for the following four purposes, when the activity history is shared with Microsoft:

1. Provide personalised experiences
2. Provide relevant suggestions
3. Improvement of (all) Microsoft products and service by applying machine-learning, and;
4. To diagnose errors and help fix them.[91]

Microsoft does not explain how these purposes relate to the other purposes mentioned in the general privacy statement but does refer to its Privacy Statement "*To learn more about how Microsoft products and services use this data to personalize experiences while respecting your privacy."*[92]

4.4 Purpose of disclosure to law enforcement

As a data controller, Microsoft may be obliged to hand over personal data to law enforcement.

In its general privacy statement, under '*Reasons we share personal data*', Microsoft explains that the company may access the contents of files on OneDrive to respond to valid legal requests from law enforcement or other government agencies

"*We will retain, access, transfer, disclose and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following:*

- *Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies."*[93]

Microsoft publishes a bi-annual transparency report. In the Netherlands, in the period January-June 2018, Microsoft received 211 requests for personal data from Dutch law enforcement authorities, relating in total to 474 unique accounts/users.[94] These requests can relate to any Microsoft consumer or business data. In an earlier dialogue about Microsoft Office, Microsoft explained that very few of law enforcement requests related to business cloud customers. 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 that organisation cannot be trusted.

[90] Ibid.
[91] Ibid.
[92] Ibid.
[93] Microsoft general privacy statement, May 2019.
[94] Microsoft Law Enforcement Requests, select Jan-Jun 2018 and apply filter to 'the Netherlands'. This shows 252 accounts/users. In the period Jul-Dec 2018 (the latest available period) there were 222 accounts/users specified in the request., URL: https://www.microsoft.com/en-us/corporate-responsibility/lerr/ (URL last visited and recorded 5 June 2019).

With regard to Online Services such as Office 365, Dynamics and Azure, Microsoft promises *"not [to] 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."* This guarantee, even though only limited to Customer Data at rest, does not apply to the Windows 10 diagnostic data.

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.

5.1 Different international Microsoft entities

In its 2017 investigation report, the Dutch DPA included an organisational chart, with the different Microsoft entities, ownership and management control.

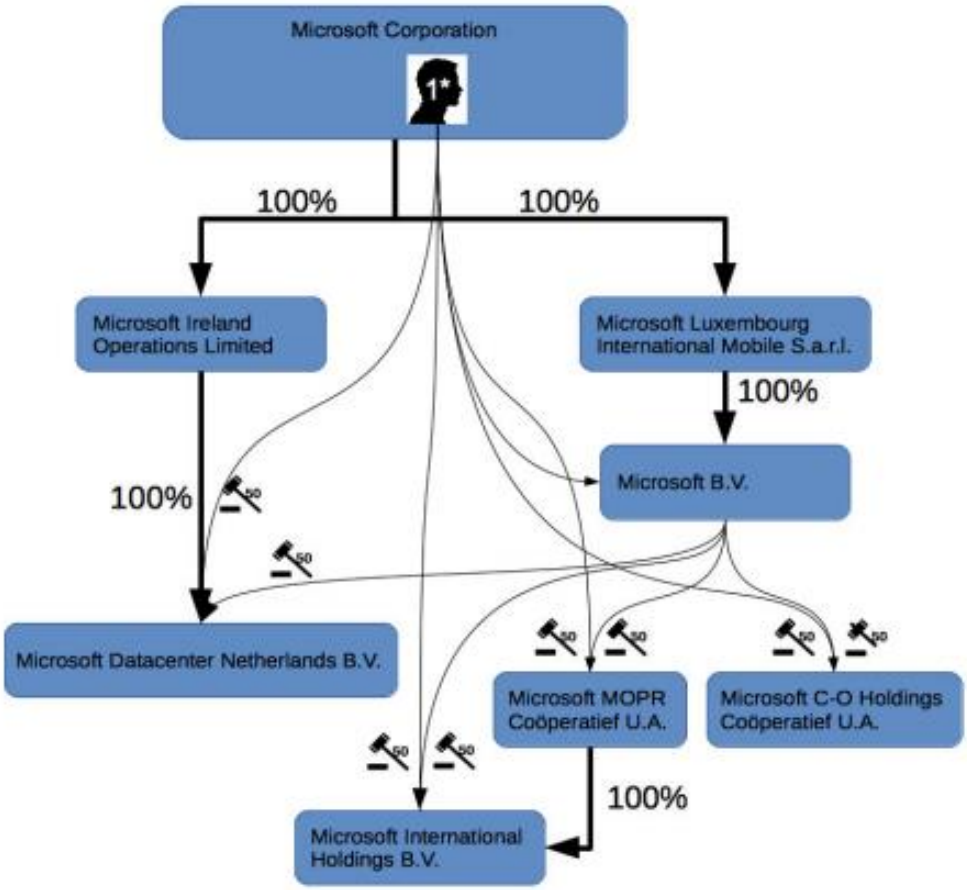
In the Windows 10 Enterprise contract structure, contracts are closed with the entity Microsoft Ireland Operations Ltd. According to Microsoft, Microsoft B.V. (the Dutch subsidiary), specifically the account team, represents Microsoft Ireland Operations Limited in relations with the Dutch government.

In all public documents, Microsoft Corporation claims to be the (sole) data controller for all data processing through Windows 10 Enterprise. According to the general (consumer oriented) privacy statement of Microsoft, the Ireland entity would be the Microsoft data controller for all users in the EU.[95]

Apparently, like many other non-EU corporations, Microsoft has confused the roles of 'lead establishment' and 'data controller in the EU'. It would make a lot of sense for Microsoft to appoint its Irish subsidiary as the 'lead establishment' in the EU, as defined in art. 4(16) of the GDPR. But it follows explicitly from the definition that the establishment itself is not the controller or the data processor.

[95] Microsoft privacy statement, May 2019, *"for those in the European Economic Area and Switzerland, Microsoft Ireland Operations Limited are data controllers for personal data we collect through the products subject to this statement."*

Figure 1: Organisational chart international Microsoft entities[96]



*Art 4(16) GDPR: '**main establishment**' means:*
*(a) as regards **a controller with establishments in more than one Member State**, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;*

*b) as regards **a processor with establishments in more than one Member State**, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;*[97]

The GDPR requires non-EU based organisations that process personal data in the context of their activities in the EU to either have one or more establishments in the

[96] Screenshot from the chart made by the Dutch DPA, findings report Windows 10 diagnostic data, p. 22.
[97] See also Art 3(1) of the GDPR: "*This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*"

EU, or a representative in the EU. By designating a lead establishment, organisations can profit from the One-Stop-Shop principle. From a data protection perspective, such a lead establishment ensures that non-EU corporations are bound by, and can be held to, European data protection standards, by a lead DPA.

It is possible that a European subsidiary also has a data controller role for specific purposes of data processing, for example if a subsidiary provides customer service to customers in the EU, or processes financial data to send invoices. But it is highly unlikely that the Irish Microsoft entity has any say at all about the nature of the processing of the diagnostic data from Windows 10 Enterprise. The data flow is sent directly to Microsoft's back-end servers in the USA, and the data are analysed by a team of USA based Microsoft engineers.

The general privacy statement and the Privacy Shield certification are signed by Microsoft Corporation. The USA mother organisation has determined, and dynamically changes, what telemetry data are collected, for what purposes, that the data are sent to servers in the USA and stored in the central database(s) in the USA, where they are analysed by 10 different USA-based teams of engineers. This was also confirmed by the Dutch DPA with regard to the consumer and Pro versions of Windows 10.[98]

The following analysis therefore only addresses the role of Microsoft Corporation as a (joint) data controller or as a data processor (not the role of Microsoft Ireland).

5.2 Microsoft's own qualification as data controller

Microsoft explicitly considers itself to be a (sole and independent) data controller for the functional and diagnostic data it collects via Windows 10 Enterprise software. Only with regard to Windows Analytics, and with regard to the Windows Defender Advanced Threat Protection (ATP), Microsoft qualifies itself as a data processor.

Microsoft explains in its public documentation:
"Controller scenario
For example, when an organization is using Microsoft Windows Defender Advanced Threat Protection (ATP) to detect, investigate, and respond to advanced threats on their networks as part of their IT operations, that organization is collecting data from the user's device – data, that might include personal data. In this scenario, the organization is the controller of the respective personal data, since the organization controls the purpose and means of the processing for data being collected from the devices that have Windows Defender ATP enabled.

Processor scenario
In the controller scenario described above, Microsoft is a processor because Microsoft provides data processing services to that controller (in the given example, an organization that subscribed to Windows Defender ATP and enabled it for the user's device). As processor, Microsoft only processes data on behalf of the enterprise customer and does not have the right to process data beyond their instructions as specified in a written contract, such as the Microsoft Product Terms and the Microsoft Online Services Terms (OST).

GDPR relationship between a Windows 10 user and Microsoft

[98] The Dutch DPA provides a detailed explanation of the roles of Microsoft Corporation, Microsoft Ireland and Microsoft Netherlands B.V. in the Windows 10 telemetry investigation report. See paragraph 2.2 and the assessment on pages 105-112 of the Dutch DPA report.

For Windows 10 services, Microsoft usually is the controller (with exceptions, such as Windows Defender ATP). The following sections describe what that means for the related data."[99]

Microsoft also mentions its position as data processor for Windows Analytics:

"As a result, in terms of the GDPR, the organization that has subscribed to Windows Analytics is acting as the controller, while Microsoft is the processor for Windows Analytics."[100]

The Windows Defender ATP service is mentioned in the Online Service Terms as one of the Core Online Services. Microsoft explains: "*Enrolled devices transmit usage data to Microsoft datacentres, where that data is analyzed, processed, and stored. The security operations center (SOC) of the organization can view the analyzed data using the Windows Defender ATP portal. As a result, in terms of the GDPR, the organization that has subscribed to Windows Defender ATP is acting as the controller, while Microsoft is the processor for Windows Defender ATP.*"[101]

This position from Microsoft is in strong contrast with its self-qualification as data processor for the diagnostic data it collects via the Office ProPlus software. As analysed in the DPIA on Office ProPlus, Microsoft only considers itself to be a data controller for the collection of personal data via and about the 'voluntary' Connected Services, such as the online spelling checker and translation service.

In response to questions of the Ministry of Justice, Microsoft wrote in March 2018: "*Microsoft does not agree with the Ministry's assessment that we are a joint controller with our customers with respect to Windows 10 data processing. Microsoft is the independent and sole controller, and Microsoft determines the ways and means of processing. Enterprise customers are given substantial choice and control over the amount of data processed, but where that data is collected by Microsoft, it is wholly within Microsoft's control and responsibility to comply with controller obligations under the GDPR.*"[102]

In the previous DPIA of June 2018 on Windows 10 versions 1709/1803, it was also concluded that Microsoft was a joint controller with the government organisations for the processing of the diagnostic data. This DPIA recommended that SLM Rijk and Microsoft should define their respective roles and the measures to guarantee GDPR compliance regarding the telemetry data in a joint controller agreement. Because Microsoft provides partial access to the telemetry data to the *administrators*, without such an agreement this access would qualify as (unlawful) further processing by a third party.[103]

The qualification of parties processing personal data has to be determined by a factual and formal analysis. The formal contractual arrangements can provide an important indication of the roles of different parties but are not leading in the analysis who determines the purposes, and to a lesser extent, the means of the data processing.

---

[99] Windows and the GDPR: Information for IT Administrators and Decision Makers, 11 May 2018.
[100] Ibid.
[101] Ibid.
[102] Microsoft Annex 2: Responses to Ministry of Justice and Security Questions, following confirmation of the outstanding questions on 28 February 2018.
[103] Windows 10 DPIA by Privacy Management Partners - in opdracht van het Ministerie van Justitie en Veiligheid, not published, p. 25.

In theory, there are 3 possible qualifications.

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

As will be explained below, the first scenario is desirable with regard to all diagnostic data collected in an Enterprise environment, regardless whether the software is Office, Azure or Windows. The third scenario (Microsoft as a unique data controller) can only theoretically apply to the collection of diagnostic data about the use of telemetry data in the Windows software. To start with, the employees as end-users do not have a contractual relationship with Microsoft, but with their employer. As will be explained below, based on a factual analysis, Microsoft and the Office Enterprise customers have to be qualified as joint controllers for the diagnostic data collected via Windows 10.

5.3 Assessment Microsoft as data processor

In this scenario, a governmental organisation deploys the Microsoft Windows 10 operating system to carry out regular work tasks. Following the definition of a data processor, Microsoft may only process the personal data necessary for the exercise of specific lawful instructions provided by the governmental organisation. In that case, Microsoft could be qualified as a processor for the organisation in question.

If the Online Service Terms would apply, Microsoft gives the strongest privacy protections to Customer Data *at rest*, if the data are provided through Core Online 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 the EU Standard Contractual Clauses. Microsoft already promises, via its Online Service Terms and the specific GDRP amendment negotiated by SLM Rijk, to not use these Customer Data for direct marketing or similar commercial purposes.

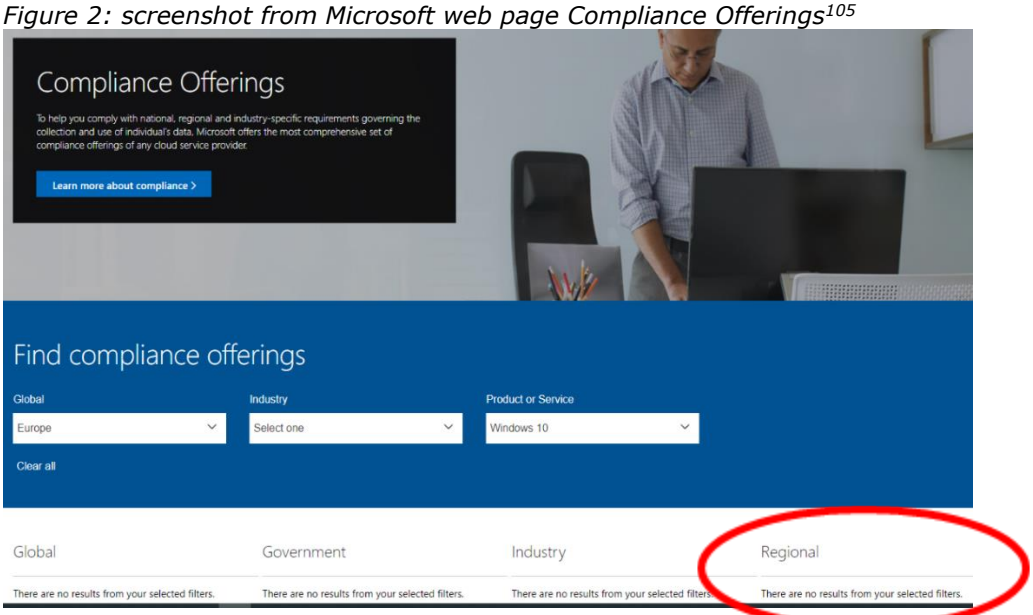
This level of data protection and these guarantees unfortunately do **not** apply to the processing of Windows 10 diagnostic data, and the cloud sync functionality of Timeline. There is no limitative list of purposes and no contractual agreement on purpose limitation. The Windows 10 software is excluded from the Online Service Terms. The only two components in Windows 10 for which Microsoft provides guarantees are the Windows Defender Advanced Threat Protection Service and Windows Analytics, but these services are tested against the requirements set forth in ISO 27001, ISO 27002, and ISO 27018, but not audited under the strict SOC-1 and SOC -2 audit regimes.[104] The transfer of personal data from these two specific components is covered by self-adherence to the Privacy Shield (and not by the EU Standard Clauses).

[104] Appendix A of the OST version February 2019 contains the OST Core Online Services, and explains that Endpoint Detection & Response, Automatic Investigation & Remediation and Secure Score are included. Microsoft provides extensive documentation about audits and compliance tests, URL: https://servicetrust.microsoft.com/ ViewPage/MSComplianceGuide (URL last visited and recorded on 20 March 2019). This information shows that only the specific Windows Defender malware software has been assessed to comply with the ISO standards 27001 en 27018.

Microsoft does not make any (other) audits available about the data processing in Windows 10 Enterprise, or other types of assessment of the compliance with the GDPR, such as a DPIA report.

The page with compliance offerings shows no results for Windows 10 Enterprise.

Figure 2: screenshot from Microsoft web page Compliance Offerings[105]



The only two types of audits that are shown for the data processing in Windows 10 if no region and no industry is selected, are the industry self-regulatory CIS Benchmark that applies to Cloud services, and the US Government cryptography standard FIP 140-2.

The CIS Benchmark only applies to Azure and not to Windows 10. The Federal Information Processing Standard (FIPS) Publication 140-2 defines minimum security requirements for cryptographic modules in products and systems. Microsoft validates the Windows 10 cryptographic modules against this standard with each new release of the Windows operating system.

Following its own qualification as a data controller, Microsoft has not concluded a data processing agreement with its Enterprise customers for Windows 10. Instead, the standard consumer-oriented privacy terms and conditions of Microsoft apply. The processing of personal data via the Windows 10 Enterprise software is not part of the contractual guarantees in the Online Service Terms and enrolment framework between SLM Rijk and Microsoft. The specific protections and limitations in the OST and GDPR amendments can only apply to a subsection of diagnostic data, -if they apply at all- if there is a hybrid deployment, and Microsoft collects diagnostic data on its own servers (via server generated event logs) about the use of Online Services such as SharePoint Online or OneDrive.

Since the OST do not apply to the Windows 10 diagnostic data, and Microsoft does not offer customers the possibility to create amendments on its general privacy terms, organisations are not able to limit the purposes for which Microsoft processes the

[105] Microsoft Trust Center Compliance Offerings, URL: https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings (screenshot recorded 20 March and 5 June 2019).

diagnostic data. It is true that Microsoft offers different telemetry settings and public information (since the spring of 2018) about the nature and amount of telemetry data. This enables organisations to minimise the processing of personal data by Microsoft, and to opt-out from certain options. However, these options do not allow the organisations to provide the legally required specific instructions wat personal data may be processed for what purposes. Adding to the confusion Microsoft uses some telemetry data for data processor services such as the Windows Defender Advanced Threat Protection.

Following a practical analysis, Microsoft cannot be qualified as a data processor. The administrators cannot fulfil their role as data controllers for the diagnostic data. It follows from section 4 in this report that Microsoft has determined the 16 general purposes of the processing outlined in its general privacy statement, the 4 purposes of telemetry at the Security level and the 4 purposes for the cloud sync functionality of Timeline.

One of the 16 identified purposes from the general privacy statement is that Microsoft allows itself to determine what other purposes may be compatible for the processing of diagnostic data. Only data controllers can determine what personal data may be processed for what purposes. A data controller may hire a technology company and outsource certain complicated data processing tasks, such as ensuring the security of the processing, or providing a well-functioning, bug free service. In order to achieve such clear objectives, the data processor has a certain liberty to decide how the personal data are processed, in what systems (with what means). But Microsoft has contractually maximised its liberty as data controller, and does not contractually limit the processing to well-defined, clearly delineated purposes that would give the government organisations the necessary control.

Other general purposes from the privacy statement are: 'personalisation', 'product development', 'advertising', 'personalised offers', 'business intelligence' and 'research'. Microsoft also mentions the use of contact data, such as email addresses, to send promotional communication. These purposes of the data processing primarily serve 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 these types of data processing.
Additionally, Microsoft itself determines the scope of the audits. If Microsoft would be a processor for the Windows 10 diagnostic data, the data controllers (in this case the Dutch government organisations) would have the right to ask for specific audits and add audit questions to existing audit frameworks.

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.[106] Article 48 of the GDPR creates an exception to this rule, acknowledging that a data processor may sometimes be forced

[106] 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*."

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.[107] So far, no such mutual assistance treaty has been negotiated between NL and the USA, or the EU and the USA. In February 2019, Commissioner Vera Jourová presented a proposal for an EU-US agreement on direct access to electronic evidence.[108] According to a news article from Bloomberg, negotiations may start in the spring of 2019.[109]

Finally, as will be described in section 10 of this DPIA, Microsoft determines the retention period for the diagnostic data, rather than the Enterprise customers. Microsoft writes: "*Customer-specific diagnostic data retention practices are not supported. The Online Services are a hyperscale public cloud delivered with standardized service capabilities made available to all customers. Beyond configurations available to the customer in the services, there is no possibility to vary operations at a per-customer level. Accordingly, we cannot support a customer-specific commitment related to storage duration for diagnostic data.*"[110]

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 the Windows 10 diagnostic data.** By taking these decisions, Microsoft acts as 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.

[107] 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.
[108] Press release European Commission, Security Union: Commission recommends negotiating international rules for obtaining electronic evidence, Brussels, 5 February 2019, URL: http://europa.eu/rapid/press-release_IP-19-843_en.htm (URL last visited and recorded on 20 March 2019).
[109] "*The European Commission wants the EU to enter into talks with the U.S., and negotiations may start this spring*" quoted in Bloomberg, Huawei Frightens Europe's Data Protectors. America Does, Too, 24 februari 2019, URL: https://www.bloomberg.com/news/articles/2019-02-24/huawei-frightens-europe-s-data-protectors-america-does-too (URL last visited and recorded on 20 March 2019)
[110] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q8 (preamble).

5.4 Assessment Microsoft and organisations as joint controllers

Following jurisprudence from the European Court of Justice, the government organisations have to be qualified as joint controllers because of their decision to use the Windows 10 software.

The European Court of Justice has clarified in two rulings[111] and an advice from the Advocate General[112] that parties may very soon be qualified as joint controllers, even when they do not have access to all the data collected by the other party, and also when the levels of responsibility are very unevenly divided. While the two rulings and the advice 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.

Windows Enterprise Customers can exercise relevant control over the processing of diagnostic data. As explained in section 3.1 of this report, admins can minimise the data processing via the Security level, and additionally switch off or block the processing of some diagnostic data, by disabling certain services. Even though this influence is limited to opt-out possibilities, 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 Windows 10 is based on the prior collection of event data from the computers or other devices of users of the Windows software, and the processing of the personal data of those users for such statistical purposes.[113]
Microsoft has confirmed in the ongoing talks with SLM Rijk it is considering the scenario for joint controllership for the processing of telemetry data from Windows 10 Enterprise. However, in case of such joint controllership, Microsoft will still have to have limit the processing to specific purposes for which either the other government controller, or Microsoft itself, has a legal ground. This will be elaborated in section B.11 of this report.

5.5 Assessment Microsoft as the sole data controller

Microsoft considers itself to be an (independent) data controller for the diagnostic data it collects via Windows 10. In practice, this situation is very unclear for the end-users of the service. Most government organisations in the Netherlands use both Windows 10 and Microsoft Office.

---

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

[112] Advocate General Bobek of the European Court of Justice, C-40/17, Fashion ID, opinion delivered 19 December 2018, ECLI:EU:C:2018:1039.

[113] 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.*

It is illogical that the Office software belongs to the (modern) Online Services for which Microsoft is a data processor, while the Windows operating system would still be an off-the-shelf consumer product. Both Office and Windows are part of Microsoft Enterprise 365 packages. From the perspective of end-users Office and Windows offer comparable, and heavily intertwined services.

As a sole data controller, because Microsoft stores telemetry data on the device and makes the software send these data to its servers in the USA, based on the Dutch Telecommunications Act, Microsoft would need to obtain specific and informed consent from the employees before processing their personal data. Other legal grounds are not available. Opt-outs cannot be qualified as consent, nor from the employees, nor from the administrators. Employees are in a dependent position from their employer and cannot refuse to use the Windows 10 operating system.

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 (SLM Rijk acting as representative of the different government organisations that procure the software). 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.

6.1 Interests Microsoft

Microsoft describes Windows as "*a personalised computing environment that enables you to seamlessly roam and access services, preferences and content across your computing devices from phones to tablets to the Surface Hub. Rather than residing as a static software program on your device, key components of Windows are cloud-based, and both cloud and local elements of Windows are updated regularly, providing you with the latest improvements and features.*"[114]

Microsoft is integrating the Windows 10 software in Microsoft Enterprise 365 packages, with an annual subscription model.[115] Microsoft has a strong economic and financial interest in transforming itself from a software company into a (subscription based) service provider. For investors, recurring revenue models mean stable and predictable recurring revenue, as opposed to estimates for one-time transactions. In order to retain customers in annual recurring revenue schemes, Microsoft has a strong incentive to gain detailed customer insight in order to cross-sell other services and market to new customers.

In its 10-K filing with the USA Sec over 2018, Microsoft describes this transformation as follows: "*We continue to transform our business to lead in the new era of the*

[114] Microsoft Privacy Statement, under the header 'Windows'.

[115] "*Microsoft 365 brings together Office 365, Windows 10, and Enterprise Mobility + Security to help organizations empower their employees with AI-backed tools that unlock creativity, increase teamwork, and fuel innovation, all the while enabling compliance coverage and data protection.*" In: Microsoft Annual Form 10K 2018, PART I, ITEM 1. BUSINESS, GENERAL, 'Embracing Our Future'. URL: https://c.s-microsoft.com/en-us/CMSFiles/MSFT_FY18Q4_10K.docx?_version=b04fa6cd-ed0e-a4ea-6f4f-05c9f644b8a2 (URL last visited and recorded on 20 March 2019).

intelligent cloud and intelligent edge. We bring technology and products together into experiences and solutions that unlock value for our customers. In this next phase of innovation, computing is more powerful and ubiquitous from the cloud to the edge. Artificial intelligence ("AI") capabilities are rapidly advancing, fuelled by data and knowledge of the world. Physical and virtual worlds are coming together to create richer experiences that understand the context surrounding people, the things they use, the places they go, and their activities and relationships. A person's experience with technology spans a multitude of devices and has become increasingly more natural and multi-sensory with voice, ink, and gaze interactions."[116]

With its pricing schemes and limitation of the support lifetime for locally installed versions of the Windows (and Office) software, Microsoft strongly encourages the Dutch government to switch from *on-premises* deployments to cloud-only services.

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, according to 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 *at rest* in specific data centres in the EU, not about other types of data, such as the diagnostic data. Microsoft argues that committing to more local or EU storage would involve high costs and be a barrier to innovation.

With the move to the cloud Microsoft is able 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, according to Microsoft.

Microsoft has explained that it competes with other large-scale cloud providers and considers it an essential economic interest to be able to process large amounts of data to develop new services. Like its competitors, Microsoft also wants to monetise user behaviour. "*Our ambition for Windows 10 is to broaden our economic opportunity through three key levers:* […, …,] *and monetization opportunities such as gaming, services, subscriptions, and search advertising.*"[117]

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 in this report, both as a data controller and as a data processor.

6.2 Interests Dutch government organisations

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.

The Dutch government also has a strong general interest in providing a reliable, always on, well integrated operating system to its employees. Well-functioning for the Dutch government also means that the software and the files processed with it, have

[116] Ibid, under 'Reinvent Productivity and Business Processes.
[117] Ibid.

to be accessible on different devices, and accessible from different locations. The ability for employees to seamlessly work at home allows the government to cut back spending on workspaces in offices. Given the interest in nomadic working, the government also needs to be able to use new tools and services that allow employees to collaborate regardless of time and place. These tools and services have to be compatible for all employees, thus creating a strong interest for government organisations to combine different Microsoft products.

The interests of Microsoft and the Dutch government align when it comes to the use of a limited set of diagnostic data to keep the services secure. As part of the shared interest in security, Microsoft needs to be able to deliver timely updates of the software.

Microsoft explains: "*Windows as a Service accelerates the cadence to provide rich updates more frequently, and these updates require substantially less effort to roll out than earlier versions of Windows. Since it provides more value to organizations in a shorter timeframe, delivering Windows as a Service is a top priority for us. The release cadence of Windows may be fast, so feedback is critical to its success. We rely on diagnostic data at each stage of the process to inform our decisions and prioritize our efforts.*"[118]

Similarly, the interests are aligned that Microsoft needs to (continuously) deliver a well-functioning OS, for the Dutch government to prevent loss of labour capacity.

6.3 Conflicting interests

However, the interests do not align when it comes to the use by Microsoft of the diagnostic data to develop new services, to detect usage of products of competitors, or to gain deeper marketing insight in current customers. These types of processing serve the commercial interests of Microsoft, while the government already pays with money for the software. These types of data processing are likely to create a high data protection risk, not only for the employees that work with the Windows 10 software, but all other data subjects whose data may be processed by government employees. The inhabitants of the Netherlands generally do not have a choice with regard to the government organisations they interact with.

7. Transfer of personal data outside of the EU

The GDPR contains detailed requirements for the transfer 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 (Privacy Shield).

Personal data may also be transferred from a data controller in the EU (a government organisation) to a (joint) data controller in a third country using the Standard Contractual Clauses, as drafted by the European Commission under the Data Protection Directive. These clauses are meant to ensure a high level of protection contractually.

[118] Microsoft, Windows IT Pro Center, Configure Windows diagnostic data in your organization, 4 April 2018.

In the Online Service Terms, Microsoft guarantees that a limited subcategory of data from the Core Services which Microsoft defines as Customer Data, will only be stored in EU data centres. There is no such commitment from Microsoft with regard to the storage in the EU of data about Windows 10. As explained in section 5 of this report, Windows 10 is not covered by the Online Service Terms, and Microsoft considers itself to be the sole data controller for all processing of personal data through and about Windows 10. The transfer of diagnostic data from the EU to the Microsoft servers in the USA is only covered by the Privacy Shield.

The Privacy Shield is an uncertain guarantee. Microsoft has certified itself under this regime.[119] There is reasonable doubt about the viability of the Privacy Shield. While the European Commission issued a review in December 2018, stating that improvements to the Privacy Shield have been made,[120] it is not clear if the agreement will be enforced.

Similarly, there is doubt about the validity of the Standard Contractual Clauses, another frequently used instrument to transfer personal data to companies outside of the EEA. The Standard Contractual Clauses have been drafted by the European Commission in 2004 (controller to controller) en 2010 (controller to processor).[121]

Both the Privacy Shield and the SCC are the subject of pending procedures at the European Court of Justice whether these instruments offer sufficient safeguards against the risks of extensive surveillance.[122]

---

[119] Microsoft is an active participant in the Privacy Shield Framework according to the searchable list of participants, URL: https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK&status=Active (URL last visited and recorded 5 June 2019).

[120] European Commission, Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield, 19.12.2018, URL: https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf.

[121] European Commission, Data Protection, Standard Contractual Clauses (SCC), URL: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (URL last visited and recorded 5 June 2019).

[122] There are two requests pending at the European Court of Justice with regard to the guarantees for the protection of personal data when transferred to the USA. The oldest request, from 9 December 2016, filed by La Quadrature du Net is case T-738/16. This case is about the validity of the Privacy Shield decision from the European Commission. The European Court will hear this case on 1 and 2 July 2019. See: https://www.laquadrature.net/en/2019/05/24/hearing-against-the-privacy-shield-before-the-general-court-of-the-eu/ (URL last visited and recorded 5 June 2019).
The other case is the procedure from Max Schrems against the Irish data protection commissioner, case C 311/18. This latter case results from a prejudicial question from the Irish High Court to the ECJ. In this case, the European Court of Justice examines the facts established in the procedure between Max Schrems and the Irish data protection supervisor. The Irish High Court held a hearing on this subject in February and March 2017. On 3 October 2017, the Irish Court ruled that the Irish regulator was right that the Standard Contractual Clauses between Facebook Ireland and Facebook Inc. in the US were invalid. The judgment of the Irish Court is available at URL: http://www.europe-v-facebook.org/sh2/HCJ.pdf. Facebook has filed an appeal with the Irish Supreme Court against this referral, but on 31 May 2019 the

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.

In the general privacy terms, under 'Where we store and process personal data', Microsoft gives a very broad description of international transfers outside of the EU: "*Personal data collected by Microsoft may be stored and processed in your region, in the United States, and in any other country where Microsoft or its affiliates, subsidiaries or service providers operate facilities. Microsoft maintains major data centres in Australia, Austria, Brazil, Canada, Chile, Finland, France, Germany, Hong Kong SAR, India, Ireland, Japan, Korea, Luxembourg, Malaysia, the Netherlands, Singapore, South Africa, the United Kingdom and the United States.* (…)."[123]

7.1 No overview of (sub-)processors outside of the EU

Via its general privacy statement, Microsoft informs users about its USA-based subsidiaries that may process the personal data. Microsoft states they all adhere to the Privacy Shield Principles.[124] Microsoft does **not** provide a public list of (sub-) processors that could process the diagnostic data from Windows 10. In the general privacy statement, Microsoft just mentions the existence of processors and that they must abide by 'our' data privacy and security purposes. This does not ensure that Microsoft only engages (sub-)processors that are legally bound to process the personal data in compliance with the GDPR.

Microsoft writes: "*We also share personal data with vendors or agents working on our behalf for the purposes described in this statement. For example, companies we've hired to provide customer service support or assist in protecting and securing our systems and services may need access to personal data to provide those functions. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose*."

8. Techniques and methods of the data processing

Microsoft collects diagnostic data through the separate telemetry client built in its operating system Windows 10.

8.1 Telemetry data

The telemetry client inside the Windows 10 software collects events with information about components of the software and stores these snapshots on the device. The

---

Irish Supreme Court has rejected this appeal. See: https://www.reuters.com/article/us-europe-privacy-ireland/irish-supreme-court-rejects-facebook-bid-to-block-ecj-data-case-idUSKCN1T112I (URL last visited and recorded 5 June 2019). The European Court of Justice will now hear this case on 9 July 2019, one week after the earlier case.

[123] Microsoft general privacy terms, last updated November 2018. Microsoft continues with an explanation that personal data are usually stored near the location of the user, with a back-up elsewhere, but this is not relevant for the diagnostic data from Windows 10, as they are directly sent to Microsofts servers in the USA.

[124] The list is available at: https://privacy.microsoft.com/nl-nl/entity-list-adhering-to-privacy-shield (URL last visited and recorded on 5 June 2019). The list only mentions names of the companies, without any indication of the nature of their business of the purposes for which they may process the personal data from government customers in the Netherlands.

client is served by the ETW providers, as explained in paragraph 2.2 of this report, based on the investigation by the German federal information security agency BSI. Microsoft encodes the telemetry data. Each encoded packet contains multiple events that occurred over a period of time. This practice reduces the number of packets that are sent from Windows to Microsoft, to limit the use of the end-user's device resources.

It is not known how frequently the different events capture data, or how frequently the client transmits the collected data to the Microsoft servers. However, the BSI report shows that the telemetry client contacts Microsoft's back-end servers twice per hour.[125] Microsoft takes note of the type of subscription plan with regard to internet usage.

Technically, the diagnostic data from the Windows 10 software are sent through one unified telemetry API to different network points. The network traffic captured by the technical lab shows that telemetry traffic is sent to (at least) 3 different network endpoints.

Table 4: network endpoints and description

Hostnames	Description
nav.smartscreen.microsoft.com	Function in the browser Edge to detect phishing and malware
web.vortex.data.microsoft.com	Diagnostic data collection through a.o. Edge
v20.events.data.microsoft.com	Connected User Experience and Diagnostic component with Windows 10 version 1803 and Azure Analytics
fe2.update.microsoft.com	Windows updates
onedriveclucprodbn20030.blob.core.windows.net	Connections to OneDrive
licensing.mp.microsoft.com	License check

At the Security level for a 'local' Windows 10 install (On Premise AD), the Data Viewer Tool shows few events. However, as BSI also has noted, there is still outgoing traffic to known telemetry endpoints for Windows, and connections to OneDrive. The difference between the Security level and the disabled telemetry, with blocking of all telemetry endpoints, is minimal. In both cases, there is still traffic with the known Office telemetry endpoints. In the 'disabled telemetry scenario, no data are sent to OneDrive endpoints, but data are still being sent to licensing.mp.microsoft.com (for a License check and to fe2.update.microsoft.com (for Windows updates).

If an organisation allows users to use Microsoft Timeline to sync their devices (and therefore, send activity history data to Microsoft), Microsoft will register what website

[125] BSI report, Work Package 4: telemetry. Executive summary in English, figures 27 and 28.

have been visited, and further process information from its cloud servers what files have been accessed. Files on the on-premise network are not captured.

8.2 Local versus hybrid installation

Enterprise customers can install the Windows software on-premise, or in combination with Online Services such as SharePoint Online. The Dutch government is testing this hybrid cloud combination. In this new set-up, the content data can be stored in Microsoft's cloud services SharePoint Online and OneDrive for Business.

From a data protection perspective, the main difference between the different Windows deployments is that users generally must have a Microsoft account in case of hybrid deployment. This is not necessary if the installation is completely local (No AD/stand-alone). In that case Microsoft does not know the local ID. However, if a user uses Office 365 ProPlus CTR, the user needs to have an Office 365 account. If a user with a local Windows account wants to use the Microsoft Store, Skype, SharePoint Online, OneDrive for Business, Exchange Online or Windows Timeline, he or she also needs to create a Microsoft account.

8.3 Dynamic big data processing

The collection of Windows 10 (and Microsoft Office) telemetry data is highly dynamic. The German information security agency BSI has observed that the configuration of the data stream changed several times per hour. This may be due to the use of specific software or apps, but it is also possible for the engineering teams to add new data and new events.

Some of the Windows 10 telemetry data are stored long term in the central Cosmos database, just like the Microsoft Office telemetry data. 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.*"[126] Microsoft explains that system-generated event logs from its cloud servers, such as SharePoint Online, are stored in Cosmos as well.[127]

Some of the purposes in the general privacy statement point to processing for yet unknown purposes (such as product development, research and business intelligence). This is a typical characteristic of big data processing, that an existing large set of data is used to examine new correlations, to answer (new) business questions, for statistical inferences and as training data for machine learning. Because Microsoft has not specified what personal data it will process for what specific and narrowly defined purposes, it cannot be excluded that Microsoft uses the diagnostic data from Windows 10 for machine learning and development of artificial intelligence. Another purpose is illustrated in an article from 2016, written by Microsoft engineers, about purposes of Windows event logging: making business decisions.

An engineer is quoted in the article: "*We developed the questions first. We said: what are the things that we want to know? What hooks do we need to put into the system and what kind of reports do we need to get back out in order to answer those*

[126] Microsoft Compliance Manager Office 365, tab 'Microsoft Managed', Control ID: 6.9.3. Accessible (with Microsoft account log-in) via the Microsoft Servicetrust dashboard, the Compliance Manager, URL: https://servicetrust.microsoft.com/FrameworkDetailV2/b3d8589d-5987-45b7-8591-235c4a2f2ca2 (URL last visited and recorded on 5 June 2019).
[127] Microsoft confidential answers 1 October 2018 to the 10 follow-up questions, answer Q4f.

questions? We didn't just take raw dumps and then try and figure out what we could learn, we were targeting specific learnings."

The article explains that these questions require combining multiple data sources to provide a recommendation or decision. Another engineer remarks: "*When you start joining it against multiple data sources, that's when you get key insights."*[128]

Unlike the contractual guarantees provided in the enrolment framework for the protection of the subset of Customer Data in Office ProPlus, cloud services such as SharePoint Online and Azure, Microsoft does not provide any guarantees with regard to marketing, behavioural advertising and profiling with regard to data resulting from the use of Windows 10. Following the general privacy statement, Microsoft allows itself to use the diagnostic data for the profiling of individual users (for example under the purpose 'Personalisation'.

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, such as BIR and the upcoming BIO), 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 Windows 10 software, however limited the collection is at the Security level. Section 5 argues that the Dutch government and Microsoft are factually 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, 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 through its telemetry client has already been extensively rejected by the Dutch DPA and therefore does not merit any further explanation in this report.

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

[128] Titus Barik, Robert DeLine, Steven Drucker, Danyel Fisher, The Bones of the System: A Case Study of Logging and Telemetry at Microsoft, ICSE '16 Companion, May 14 - 22, 2016, Austin, TX, USA, p. 8-9, URL: https://dl.acm.org/citation.cfm?doid=2889160.2889231 (URL last visited and recorded on 20 March 2019).

Regulation will also broaden its scope to other providers of communication services. Microsoft and the government organisations therefore also have to take the (existing) 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. The proposed Article 8(1), Protection of information stored in and related to end-user's 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. 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
(iii) it is not further used for monitoring the employee.

The Council of ministers has been debating the proposal since October 2017. In October 2018 the ministers proposed 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;

The Council has also proposed 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 has proposed 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*[129] *having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service. In such case, consent needs to be obtained from the individual concerned.*

In the document with results of deliberations in the Council, published on 4 February 2019, a further explanation is added to recital 21, with reference to the need to respect the rights of employees as defined in the GDPR and employment law. [130] In the last publicly available document of 13 March 2019 this reference has been removed. The recital now only refers to consent from end-users, without acknowledging the difficulty of obtaining consent from employees.[131]

10. Retention Period

Microsoft does not specify the specific retention periods for the Windows telemetry diagnostic data. As a general rule, Microsoft retains the data for a period of 30 days, but some information may be retained for an unspecified 'longer' period of time.

Microsoft explains: "*Microsoft believes in and practices information minimization. We strive to gather only the info we need and to store it only for as long as it's needed to provide a service or for analysis. Much of the info about how Windows and apps are functioning is deleted within 30 days. Other info may be retained longer, such as error reporting data or Microsoft Store purchase history*."[132]

In its general privacy statement, under the header of 'Our retention of personal data', Microsoft indicates that it stores personal data "*as long as necessary to provide the products and fulfil the transactions you have requested, or for other legitimate purposes such as complying with our legal obligations, resolving disputes and enforcing our agreements.*"

Microsoft mentions six criteria that may determine the retention period. Three relevant criteria are:

---

[129] In the 13 March 2019 version the word 'entity' is replaced by 'person'.
[130] Council of the European Union, Interinstitutional File 2017/0003, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5934_2019_INIT&from=EN (URL last visited and recorded 5 June 2019).
[131] Council of the European Union, Interinstitutional File 2017/0003, ST 7099 2019 REV 1, URL: https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=consil:ST_7099_2019_REV_1 (URL last visited and recorded 5 June 2019).
[132] Microsoft, Windows IT Pro Center, Configure Windows diagnostic data in your organization, 4 April 2018.

- *"Is there an automated control, such as in the Microsoft privacy dashboard, that enables the customer to access and delete the personal data at any time? If there is not, a shortened data retention time will generally be adopted.*
- *Is the personal data of a sensitive type? If so, a shortened retention time would generally be adopted.*
- *Has Microsoft adopted and announced a specific retention period for a certain data type? For example, for Bing search queries, we de-identify stored queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers after 18 months."*[133]

An example of a specific retention period applies to the personal data processed for Windows Timeline. Microsoft explains: "*If you selected the* ***Send my activity history to Microsoft*** *check box and you were unable to finish before you had to leave the office for the day, not only would you see that Word activity in your timeline for up to 30 days, but you could also resume working on it later from another device.*[134]
Microsoft allows users to delete their activity history from their device, to stop sending their activity history to Microsoft and to clear individual activities, all activities from an individual day, or delete all activities.[135]

With regard to the telemetry data, the Dutch DPA noted in its investigation of Windows 10 Home and Pro that Microsoft applied data retention periods of 30 days, or 13 months or 37 months[136]

Microsoft explains that the administrators 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.*"

In 2017 it was not possible for users to exercise their right to have their personal data deleted. Since April 2018, Windows 10 includes a function that allows users to individually delete the diagnostic data relating to them.[137] This delete-option does not include back-ups.

Microsoft has explained that it does not make backups the way people usually understand back-ups, as passive copies, possibly even on tape. Microsoft does real-time active-active replication, with a small delay in replication. Within a period of time, the other copy would get the same delete instructions. 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.

---

[133] Microsoft privacy statement, May 2019.
[134] Microsoft, Windows 10 activity history and your privacy, 10 April 2019.
[135] Ibid.
[136] Dutch DPA, report of findings Microsoft Windows 10 diagnostic data processing, p. 7
[137] See for example: Windows Central, How to review and manage diagnostic data on Windows, 10 April 2018 Update, 1 May 2018, URL: https://www.windowscentral.com/how-view-and-manage-diagnostic-data-windows-10-april-2018-update (URL last visited and recorded on 20 March 2019).

SharePoint Online does not perform system-level backups. Daily incremental and weekly full backups are conducted for SQL Server schemas, and Active Directory information is backed up through replication across sites and datacentres. SQL Server schemas are stored for no less than 30 days and geo-replicated to alternate datacentres for high availability.

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

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 factually are joint controllers for the processing of all Windows diagnostic data. Even though Microsoft claims to be the sole data controller for the Windows diagnostic data, government organisations enable Microsoft to process the diagnostic personal data about their employees and other data subjects. Following the jurisprudence of the European Court of Justice about joint controllership (as explained in section A5 of this report), the government institutions are responsible, together with Microsoft, for the processing of personal data about the use of Windows 10 OS. Additionally, government organisations are able to influence the categories of data and purposes, as well as the retention period, by blocking or limiting the outgoing telemetry traffic and by deleting diagnostic data about users.

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 (lifesaving) interest in the processing of the diagnostic data.

Microsoft does not specify the legal grounds for the processing of diagnostic data in its general privacy statement.

11.1 Consent

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

Regardless of the role of Microsoft as a sole controller, or as a joint controller with the government organisations, this legal ground cannot be successfully invoked by either party. Nor Microsoft nor the government organisations currently ask for consent from the employees for the processing of the telemetry data, nor from the other data subjects whose data may be processed through the diagnostic data. But even if they would, such consent would not meet the criterion of 'freely given'.

For employers, it is almost impossible to obtain valid, freely given consent from employees, given the clear imbalance in the labour relationship.

Microsoft as a (sole) controller would have to prove that the processing of diagnostic data for all 16 purposes meets the strict necessity requirement laid down in Article

7(4) GDPR. 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, Microsoft does not meet the requirements of specific and informed consent. This applies both to the telemetry data and the Timeline data.

Though Microsoft provides a description of the purposes for Security level telemetry data, this does not equal a limitative list purposes for the different telemetry events such as Microsoft provides for telemetry at the Basic level.

With regard to the cloud Timeline, Microsoft does seek consent of the employees, but without informing them what personal data will be processed for what purposes. In section 4.3 of this report, four purposes have been identified for which Microsoft processes the Timeline data if a user has switched the cloud functionality On. These purposes are:

1. Provide personalised experiences
2. Provide relevant suggestions
3. Improvement of (all) Microsoft products and service by applying machine-learning, and;
4. To diagnose errors and help fix them.[138]

Because data subjects are not informed in advance, in a clear and understandable manner, what these purposes entail and how this relates to the other purposes mentioned in Microsoft's general privacy statement, and there is no information available what personal data are processed for these purposes, the consent is nor informed nor specific. However, given the sensitive nature of these data (web surfing, names of files and file paths) and the circumstance that Microsoft can provide Windows 10 without this service, there is no other applicable ground for the processing of these data.

Consent is also the only available legal ground with respect to the spirit of ePrivacy legislation. 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 or obtain consent from the end-users. Though this rule does not yet technically apply to Microsoft's monitoring of diagnostic cloud data via Windows 10, it is likely that this principle will be extended to other providers of communication services such as Microsoft in the new ePrivacy Regulation. This would make consent of the employees the only option to legitimise the processing of metadata for the Timeline functionality.

11.2 Processing is necessary for the performance of a contract

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

Employees are generally not given any choice by their government employers when it comes to the operating system they must use. The vast majority of government

[138] Microsoft, Windows 10 activity history and your privacy, 10 April 2019.

employees spends many hours each working day with a device running the Windows operating system.
Hence, to the extent that the processing would be limited to strictly necessary purposes for the performance of the contract which the data subject has with the governmental organisation, both that organisation and Microsoft as joint controllers could successfully appeal to this legal ground.

This legal ground can only apply to a limited set of personal data, for a limited set of purposes that are necessary in relation to each user, such as the need to keep Windows secure and deliver timely security updates at the Security level. The list of specific legitimate purposes for the processing of telemetry data at the Security level, as based on Microsoft's own technical purpose descriptions, would look as follows:

1. Providing the customer with the latest security updates
2. The configuration of the telemetry pipeline

Microsoft processes the Security level data for two other purposes, namely:

3. Detection and removal of malicious software
4. Windows Defender anti-virus and endpoint security protection

However, the processing for these latter two purposes can be switched off by the administrators, as described in paragraph 3.1 of this DPIA report.

If a controller is able to offer users a possibility to opt-out from certain data processing, this is evidence that the data processing is not strictly necessary to fulfil the contract with that individual user. In such cases, the legal ground of art. 6(1)b does not apply, but sometimes the legal ground of art. 6(1)f can be invoked.

The European Data Protection Board writes in its draft guidelines on the legal ground of necessity for a contract: "*A controller can rely on Article 6(1)(b) to process personal data when it can, in line with its accountability obligations under Article 5(2), establish both that the processing takes place in the context of a valid contract with the data subject* ***and that processing is necessary in order that the particular contract with the data subject can be performed*** [emphasis added for this DPIA report].[139]

Microsoft does not limit the processing of diagnostic data at the Security level to the four specific purposes described in paragraph 4.2 of this DPIA report. Legally, Microsoft permits itself to process all personal data, including the diagnostic data, for all 16 purposes in its general privacy statement. The processing for all these other purposes is not strictly necessary for the performance of the contract (from government) with the user.

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).

[139] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version for public consultation published 12 April 2019, URL: https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_en [URL last visited and recorded on 5 June 2019].

11.3 Processing is necessary to comply with legal obligation

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

This legal ground cannot successfully be invoked by either Microsoft or the government organisations for the processing of the diagnostic data about Windows 10 Enterprise. To the extent that an employer would need to use log files to detect for example data breaches or seek evidence of improper behaviour by employees, such purposes could be covered, if proper guarantees are present, by the legal grounds of e or f, necessity for the public interest, or more likely, necessity for a legitimate interest.

11.4 Processing is necessary for the public interest

Article 6 (1) (e) GDPR reads: "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*"

This legal ground is not applicable either to the diagnostic data processing described in this report, 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.

Since Microsoft is not government, nor a public organisation, it can never rely on this legal ground.

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

Article 6(1) f GDPR 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.*"

Both the Dutch government organisations and Microsoft may process a limited set of diagnostic data on the basis of necessity for their legitimate interest. At the Security level this includes processing of diagnostic data to determine what security updates to serve, to detect and remove malicious software and to apply Windows Defender anti-virus and endpoint security protection.

This does not include any of the other purposes for which Microsoft legally, according to the general privacy statement, allows itself to process the diagnostic data and the synced Timeline data.

Absent clear purpose limitation, a limitative list what diagnostic data can be processed for narrowly defined purposes, it has to be assumed that diagnostic data can be processed for all 16 purposes mentioned in Microsoft's general privacy statement, including personalised advertising and direct marketing. Such personalisation can be based on visited URLs, if the Timeline cloud sync functionality is switched on.

Following the order of the Dutch government DPIA model, the necessity of the processing is separately assessed in section 14 of this report. However, in anticipation of this assessment, 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 an entity programs a device to give access via the internet to stored data on the device. Preceding the analysis of necessity, the special character of the telemetry data and the ePrivacy consent requirements preclude the processing for most of the purposes mentioned in the Microsoft general privacy statement without the explicit consent of the end-user. As analysed above, employees are not free to give consent for other purposes.

In sum, based on the ePrivacy Directive consent is required for most of the purposes of the processing of telemetry data collected on the end-user devices, but as joint controllers Microsoft nor the government organisations can obtain valid consent given the dependency in the relationship between employees and employers.

As outlined above, a limited set of telemetry data may be processed by government organisations based on the necessity to perform a contract, or by either party based on the necessity for a legitimate interest. But to successfully appeal to these legal grounds, it is essential to contractually limit the purposes for which they must be processed. Given the sensitive character of the Timeline data, this precludes further processing for most of the current purposes (except for 'technically transmitting data to provide the service').

12. Purpose limitation

Article 5(1) b of the GDPR obliges data controllers to comply with the principle of purpose limitation. 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.*"

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.

12.1 Insufficient contractual guarantees

As explained in the sections 4 and 5 of this DPIA report, Microsoft does not offer adequate contractual guarantees with regard to purpose limitation. The Dutch government has an extensive contractual enrolment framework with Microsoft. This includes GDPR amendments on the Online Service Terms, with the purpose to ensure the exclusion of commercial use or further processing for other purposes of personal data from and about employees that use Microsoft products. But since the Online Service Terms do not apply to Windows 10 Enterprise, there are no other binding legal guarantees outside of the general privacy statement that limit the purposes for which Microsoft processes the diagnostic data resulting from the use of Windows 10.

Though Microsoft mentions four specific purposes in its technical documentation about telemetry at the Security level, and four purposes for the processing of the Timeline data, these explanations are never exhaustive. The informative texts about telemetry and Timeline are not legally binding and can be changed any time without prior warning.

Microsoft offers no contractual commitments that limit the processing of the telemetry data to the four specific purposes suggested in section 11 (Purpose limitation) in this DPIA report. Thus Microsoft can process the diagnostic data for all 16 purposes mentioned in its general privacy policy.

As described in section 4.3, Microsoft mentions four different purposes for the processing of diagnostic data for its cloud Timeline service, including the very broad purpose of improvement of (all) Microsoft products and service by applying machine-learning.

12.2 Further processing for incompatible purposes

Purpose limitation is the most difficult principle to comply with in *big data* processing. Further processing for research purposes (as mentioned in the general privacy statement) 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. Such guarantees are not provided by Microsoft.

Microsoft explicitly reserves the right in its general privacy statement to process data for *uses compatible with providing the service*. As explained in section 4.1 of this DPIA report, the purpose 'providing the service' already includes a large number of commercial purposes. These commercial purposes may provide desirable results and insights for Microsoft but are not strictly necessary to provide the service.

13. Special categories of personal data

As explained in section 2 of this DPIA, it is unlikely that the diagnostic data at the Security level contain special categories of data.

If users are not prohibited from sending their activity history to Microsoft, the company collects and stores the web surfing behaviour for a period of 30 days. Microsoft can use the visited URLs to infer special categories of data.

The processing of special categories of data is prohibited by the GDPR, unless a specific legal exception applies. The processing of these 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) by default presents high risks for the data subjects. This risk is aggravated because of the commercial purposes for which Microsoft allows itself to process the online Timeline data.

In view of the assessment in paragraph 11 of this DPIA that employees are not in a position to freely give consent to Microsoft or their employer for this type of data processing, there are no apparent exceptions on the prohibition on the processing of these personal data.

14. Necessity and proportionality

14.1 The principle of proportionality

The concept of necessity is made up of two related concepts, namely proportionality and subsidiarity. The personal data which 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 fewer 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.

14.2 Assessment of the proportionality

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

To assess whether the processing is proportionate to the interest pursued by the data controller(s), the processing must first meet the principles of article 5 of the GDPR. As legal conditions they have to be complied with in order to make the data protection legitimate.[140]

Adherence with the principle of purpose limitation has been separately addressed in section 12 of this report. Absent an exhaustive list of specific and legitimate purposes, the processing cannot be qualified as proportionate as the interests cannot be balanced.

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.

Microsoft does not publish a limitative list of events collected at the Security level. Therefore the scope of the processing is not sufficiently transparent for users and administrators. Even though Microsoft collects very few telemetry data at the Security level, not all observed events are obviously necessary to achieve the stated purpose *to keep Windows devices, Windows Server, and guests protected with the latest security updates*. For example, the event DxgKrnlTelemetry.GPUAdapterInventoryV2 provides information about the graphic processor. Microsoft describes the purpose of

[140] According to consolidated case-law from the European Court of Justice, all data processing must first meet with the principles, and second, have a legal ground. See for example C-131/12 (par 71), C:2003:294 (par 65), C-468/10 and C-469/10 (par 26).

this category of events as: "*this event sends basic GPU and display driver information to keep Windows and display drivers up-to-date.*"[141]

If an organisation has a hybrid network set-up, and users are not prevented from sending their activity history to Microsoft, the company can also collect information about the names and storage path of documents in SharePoint Online and OneDrive. Such data may be confidential / restricted or even state secret. As assessed in section 12 of this report, Microsoft legally permits itself to process these data for broad purposes such as direct marketing, product innovation and product development, including the use of training data for machine learning. These broad purposes are not immediately obvious to users, as they are not available in one place. Thus, the current processing is not transparent enough. Nor does the processing for all 16 purposes mentioned in the privacy statement meet the requirement of necessity.

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 a 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 the telemetry data, nor for some other default settings, as explained in section 3 of this report.

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 requires the deletion of personal data as soon as they are no longer necessary to achieve the purposes 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).

Microsoft stores the cloud Timeline data for a period of 30 days and allows users to selectively or collectively delete the data. This is in line with the storage limitation principle.

Microsoft does not provide public information or contractual guarantees with regard to the retention periods of the Windows 10 diagnostic data. According to the investigation report published by the Dutch DPA, Microsoft retains the diagnostic data between 30 days, 13 months and 37 months. Though users can delete diagnostic data, this does not apply to the long-term storage of diagnostic data. Since Microsoft has not provided a clear explanation about the necessity of the retention of the telemetry data at the Security level, not even for the minimum period of 30 days, the

[141] Microsoft, Windows IT Pro Center, Windows 10, version 1903 basic level Windows diagnostic events and fields, 23 April 2019.

current practice cannot be qualified as being in line with the data minimisation principle.

14.3 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 Windows 10 for most Dutch government organisations.

In practice, government organisations have been working for a very long time with Microsoft products. They have organised their work processes and development to integrate with the Windows and 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 cloud providers such as Google, or open source operating systems such as iOS, Linux or Unix 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 source operating systems would present serious difficulties for the employees. It would also take a long time to test the security and privacy aspects of a new platform, and to migrate all users and data to the new environment.

Added to that there are the costs of migrating existing content, and redevelopment of specific applications that interact with the Windows software. This situation can also be described as vendor lock-in.[142]

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.

Since the April 2018 versions of the different Windows 10 products (Home, Pro and Enterprise), Microsoft has made serious improvements to the privacy settings of the software. Microsoft has added public documentation about the contents and purposes of telemetry events at the Basic level and an option in the software to delete historical telemetry data. Additionally, Microsoft has provided group policies and registry key settings to admins of Windows 10 Enterprise, to block the telemetry data flow.

[142] See for example of the principle of vendor lock-in the explanation on Wikipedia, URL: https://en.wikipedia.org/wiki/Vendor_lock-in (URL last visited and recorded on 20 March 2019). See specifically about the risks for governments in the EU of Microsoft vendor lock-in: Computer Weekly, Locked in by choice: How European governments are handling their Microsoft addiction, 4 May 2017, URL: https://www.computerweekly.com/feature/Locked-in-by-choice-how-European-governments-are-handling-their-Microsoft-addiction (URL last visited and recorded on 20 March 2019) and TheNextWeb, Europe is living under Microsoft's digital killswitch, 10 May 2017, URL: https://thenextweb.com/eu/2017/05/10/europe-is-living-under-microsofts-digital-killswitch/ (URL last visited and recorded on 20 March 2019).

Microsoft provides users with the right to access the diagnostic data stored on their device, to individually view data on their Timeline, and to access some other data collected via Windows 10 via the Privacy Dashboard.[143]

In a hybrid networking environment, when employees choose to send their activity history to Microsoft for Timeline, the further processing of diagnostic data about file names and folder locations from SharePoint Online and/or OneDrive may cause extra data protection risks for some employees. For example, if they regularly work with classified information, the collection of extra data about their usage of certain files and documents may lead to increased risks of social engineering/spear phishing and even stalking. Or if they visit webpages that may reveal special categories of data. As described in section 10 of this report, users have the ability to individually or collectively delete data from their Timeline.

Employees have a right to data portability, if their personal data are processed based on the necessity for the government organisation to execute the (labour)contract. As outlined in the table in section 11 of this report, the data processing for 2 purposes can be based on this legal ground, namely,

1. Providing the customer with the latest security updates
2. The configuration of the telemetry pipeline

However, the government organisations (as joint controllers) may also decide to rely on the legal ground in art. 6(1)f for these and the other two purposes. This would pre-empt the right to data portability.

[143] Microsoft privacy dashboard, URL: https://account.microsoft.com/account/privacy (URL last visited and recorded 5 June 2019).

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 processing by Microsoft of diagnostic data for its own purposes can be divided in two categories: data about the behaviour of employees and content data (file names and locations)

16.1.1 Data about the behaviour and preferences of employees

With the telemetry set at the Security level, Microsoft collects a very limited amount of information, without content data or data that are otherwise confidential or sensitive. Generally, this data processing poses little risk for the data subjects that these data are used to profile or embarrass them.

However, in view of the long retention period for telemetry data (up to 37 months), the dynamic nature of the telemetry collection process, and the lack of contractual purpose limitation, it is not possible to exclude all data protection risks for the individuals concerned.

16.1.2 Content (document titles and web surfing)

If the organisation has a hybrid set-up with SharePoint Online or OneDrive, and users share their activity history with Microsoft, the company can process sensitive data such as web surfing behaviour, the titles of documents and their storage locations in SharePoint Online.

With regard to these cloud Timeline data, even though the retention period is limited to 30 days, there are some real and serious data protection risks for the employees. The fact that Microsoft processes these data without contractual purpose limitation could mean that Microsoft uses these data to draw conclusions for personalised offers and suggestions. The idea of being observed for these purposes may lead to slight embarrassment, shame, and/or to a chilling effect on the freedom to seek information.

There is an additional risk for some types of government employees if the further processing by Microsoft of the Timeline data about file and folder names in its cloud servers reveal that these employees 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.

Behavioural patterns from the Timeline data 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.

In view of these risks, SLM Rijk recommends that government administrators disable Timeline completely and prohibit users from exercising a choice with regard to this data processing. Microsoft has provided information about two Group Policies for administrators to manage these settings: Publish User Activities[144] and Upload User Activities.[145] Alternatively, administrators my want to use a Registry Key.[146]

This assessment continues with the assumption that Timeline is switched Off.

16.2 Assessment of Risks

The risks (from the processing of the diagnostic data) 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 control: Microsoft as a data controller

As analysed in section 5 of this DPIA report, Microsoft incorrectly assumes the role of (sole) data controller for the processing of the diagnostic data from Windows 10 Enterprise. A factual analysis shows that Microsoft and the government organisations should be qualified as joint controllers. Article 26 GDPR requires that joint controllers create contractual arrangements to divide responsibilities and provide clear

[144] Microsoft, Policy CSP - Privacy, Privacy/PublishUserActivities, 14 August 2018, URL: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-privacy#privacy-publishuseractivities (URL last visited and recorded on 20 March 2019).
[145] Ibid., Privacy/UploadUserActivities, URL: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-privacy#privacy-uploaduseractivities (URL last visited and recorded on 20 March 2019).
[146] Explanations about the registry keys can be found at for example Winaearo, URL: https://winaero.com/blog/disable-timeline-windows-10-group-policy/ (URL last visited and recorded 5 June 2019) and Tenforums, URL: https://www.tenforums.com/tutorials/100341-enable-disable-collect-activity-history-windows-10-a.html (URL last visited and recorded 5 June 2019). These settings have not been tested for this DPIA.

information to end-users about these arrangements. There is no such contractual agreement that outlines what personal data Microsoft may process, for what purposes. Based on its general privacy statement, Microsoft feels legitimated to process the diagnostic data for 16 purposes, including targeted advertising and personalisation.

The current positioning as a data controller results in a lack of legal grounds for most of the purposes for the diagnostic data processing in Windows 10 Enterprise. This causes a risk for government organisations, of loss of confidentiality, unlawful (further) processing and reputation damage.

As analysed in section 11 of this report, Microsoft and the government organisations do not have a legal ground for the processing of the data collected at the Security level for all the 16 purposes mentioned in the general privacy statement.

The likelihood of the risks of loss of control and unlawful (further) processing is 100%, as this report identifies that, due to the lack of purpose limitation, nor Microsoft nor the government organisations have a legal ground for most of the purposes for which Microsoft allows itself to process the diagnostic data. This risk assessment has to consider that employees are in a dependent position and cannot refuse to use the Windows 10 Enterprise software.

However, because the Security level data are minimal and do not contain sensitive data, the severity of the impact on data subjects can be qualified as low.

As a side note, concluding a joint controller agreement would only be a cosmetic measure. Such an arrangement will not solve the fundamental problem of lack of control for the government organisations. It. In order for government organisations to be in control and limit the data processing to the strictly necessary minimum, the only acceptable role for Microsoft is a role as data processor. This in turn requires a major overhaul of the enrolment framework, since some of the current GDPR compliance guarantees have already been qualified as insufficient in the Office ProPlus DPIA report.

16.2.2 Lack of control over third parties/processors and audits

As assessed in the sections 4 and 5 of this DPIA report, Microsoft provides no, or very weak contractual assurances for compliance of the Windows 10 data processing with the GDPR. The government organisations are treated on an equal level with all consumers globally, and Microsoft applies the very broad purpose descriptions in the general privacy statement.

Microsoft apparently has never audited the diagnostic data processing via Windows 10 Enterprise or has not made the results publicly available. Microsoft has not published a DPIA report about the risks of the processing of diagnostic data from Windows 10 Enterprise. Government organisations have no insight in the rules governing access to the personal data stored in Microsoft's databases, nor insight if these rules are complied with, and how compliance is monitored.

Different from the Standard Contractual Clauses provided for the diagnostic data processing in Office ProPlus, SLM Rijk does not have a specific contractual right to have audits performed or add specific questions relating to for example the contents of the telemetry data stored in the long term database, the access to these data,

monitoring of the log files with regard to access, and the further processing of these data.

This means that SLM Rijk is insufficiently able to verify compliance of the actual data processing. Additionally, Microsoft does not provide a list of processors, or 'affiliates. This means SLM Rijk and the individual government organisations that use Windows 10 have no means to verify the integrity and GDPR compliance of these processors.

Further risks are caused by the possibility that Microsoft allows third parties to process personal data, while there is no contractual guarantee that such third parties are bound to the confidentiality requirements of a data processor as defined in the GDPR.

Given the lack of information about third parties that may process the Windows 10 personal diagnostic data, and the lack of effective control of contractual promises through audits, and the fact that SLM Rijk cannot force Microsoft to stop the cooperation with one or more specific processors, the data protection risks must be assessed as reasonably likely to occur, while the possible harm at the Security level can still be qualified as low.

16.2.3 Transfer of personal data outside of the EEA

The automatic transfer of diagnostic data from Windows 10 Enterprise to Microsoft's back-end cloud servers in the US entails a risk for unlawful processing, since the United States do not have privacy legislation that offers an adequate level of data protection as defined in the (European) GDPR.

Different from the guarantees Microsoft offers in its Online Service Terms with regard to Office ProPlus with regard to storage in datacentres in the EU of user provided content, there are no contractually binding limits to the transfer of Windows 10 diagnostic data.

a) The standard of protection of personal data in most countries in the world is lower than in the European Economic Area. While Microsoft undertakes in its general privacy statement 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 or by a data processor in a third country, can be accessed by local governments.

b) Microsoft transfers the personal data from Windows 10 Enterprise to the United States under the terms of the EU-US Privacy Shield Framework. Microsoft has self-certified under this regime. There is reasonable doubt about the viability of the Privacy Shield. While the European Commission issued a review in December 2018, stating that improvements to the Privacy Shield have been made, it is not clear if the agreement will be enforced.

Microsoft applies another guarantee for the transfer of personal data collected through the use of its Online Services (such as Office, Azure and Dynamics), namely the Standard Contractual Clauses (also called "Model Clauses"). These clauses, drafted by the European Commission in 2010, allow a non-EU company to receive personal data from a company the EU.

As outlined in section 7 of this report, both the Privacy Shield and the SCC are the subject of pending procedures at the European Court of Justice whether these instruments offer sufficient safeguards against the risks of extensive surveillance.

c) The 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. Because there is no mutual assistance treaty between NL and the USA, or the EU and the USA, Microsoft risks a violation of Article 48 of the GDPR when ordered to hand over data from Dutch government organisations.

16.2.4 Long retention period

The Windows 10 telemetry data are stored for 30 days, or 13 months, or 37 months in the central Cosmos database in the USA.

Since the April 2018 versions of Windows, Microsoft includes a possibility for users to delete historical diagnostic data per device ID. This is a good remedy, but there are two remaining issues with the retention period.

First, the deletion option does not apply to data that Microsoft may incorrectly qualify as anonymous, or to the diagnostic data that Microsoft collects on its own servers in system generated event logs in case of a hybrid network set-up (with SharePoint Online and/or OneDrive).

Second, the individual opt-out does not solve the principal issue that Microsoft needs to determine what personal data necessarily need to be processed during what maximum period of time. The retention periods of 13 or 37 months seem excessive, pending evidence of the necessity, as should preferably be confirmed by an independent audit.

The risks resulting from such a long retention period are 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 the diagnostic data at Security level do not contain sensitive personal and/or confidential data, the potential harm can be qualified as low.

16.3 Summary of Risks

These circumstances lead to the following low data protection risks for the processing of Security level telemetry data:

1. Lack of purpose limitation and legal grounds for most of the purposes for the data processing.
2. Lack of control over third parties/processors and audits
3. The transfer 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
4. The long retention period of diagnostic data

Based on the ICO model, this results in the following matrix:[147]

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

[147] 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/ (last visited and recorded on 20 March 2019).

Part D. Description of risk mitigating measures

Following the Dutch government DPIA model, Part D describes the proposed measures to counter the possible negative impact and risks connected to the examined data processing.

However, in this DPIA some risk mitigating measures have already been taken for granted in the determination of the scope. This applies to the measure to set the telemetry level to Security. This also applies to the measure to turn off the new Windows Timeline functionality.

In previous Windows 10 Enterprise versions admins could not use Windows Update for Business or Intune, because this was only possible with telemetry set to Basic or higher.[148] If admins upgrade to the new 1903 version, released end of May 2019, it is possible to use Windows Update for Business with the telemetry set to the Security level.[149]

The following section therefore only discusses some additional measures to remove the remaining low data protection risks.

17. Additional risk mitigating measures

Three of the four identified low risks related to the processing of the Security level telemetry data can be removed through contractual measures. The fourth risk may be mitigated with a combination of technical and organisational measures.

As outlined in section 5 and in sections 11 and 12, it would be preferable if Microsoft would act as a data processor, and only process the diagnostic data for specific legitimate purposes, as instructed by the data controllers (the government organisations).

The lack of control over third parties and lack of audits on the factual data processing can equally be remediated through contractual measures. Such an audit could also help determine the necessary period for which the diagnostic data can be stored.

The fourth risk related to the transfer of personal data to the US, is the topic both of negotiations between the EU and the US in the context of the e-Evidence framework, and of two procedures at the European Court of Justice. Pending the outcome of these developments, Dutch government organisations should carefully consider if they can apply technical measures (such as encryption) to the contents of very sensitive and/or highly confidential/secret data if they use Microsoft cloud services such as SharePoint Online or OneDrive. They may also want to consider other organisational measures to prevent possible unlawful access, such as a policy not to include personal or confidential data in names of files and folders.

Some additional data protection risks related to the use of the Windows operating system described in this DPIA can be mitigated with technical measures by the

[148] Microsoft, Manage software updates in Intune, 12 February 2019, URL: https://docs.microsoft.com/en-gb/intune/windows-update-for-business-configure (URL last visited and recorded on 5 June 2019).

[149] Microsoft techcommunity, What's new in Windows Update for Business in windows 10, version 1903, 21 May 2019.

administrators of the government organisations. The admins should use group policies or registry keys to turn off privacy-invasive components in the operating system when the data processing is not necessary for the work of the employees.

Table 5: Risks and mitigating measures by Microsoft and government organisations

Nr	Risk	Possible measure Microsoft	Recommended measure gov organisations
1	Lack of legal grounds and purpose limitation.	Become a data processor, major overhaul of the OST.	Select Security level or block telemetry traffic.
		Provide a limitative overview of the necessary events and their content at the telemetry Security level.	Prohibit the use of Windows Timeline by centrally switching off 'publishing of User Activities' in Local Group Policy Editor or Registry Key.
		Provide a limitative overview of the specific legitimate purposes for which Timeline data are processed.	Consider creating a policy not to use personal or confidential data in file or folder names.
		Provide a separate opt-in for the collection of web surfing behaviour.	Create or revise internal data processing rules with regard to employee data, specific rules for web surfing behaviour.
2	Lack of control over third parties /processors and audits	Organise high quality audits on compliance, conduct (or publish the results of) a DPIA on the diagnostic data processing, allow government organisations to add specific audit questions.	Apply technical measures (such as encryption or use of stand alone computers) to the contents of very sensitive and/or highly confidential/secret data when the organisation uses cloud services such as SharePoint Online or OneDrive.
3	The transfer of data outside of the EEA	New contractual guarantees such as Standard Contractual Clauses or Binding Corporate Rules and/or storage of diagnostic data within the EU.	In addition to the technical measures described under 2, consider organisational measures to prevent possible unlawful access, such as a policy not to include personal or confidential data in names of files and folders.
4	The long retention period of diagnostic data	Determine, enforce and supervise compliance with necessary retention periods.	Encourage employees to use the right to delete historical diagnostic data.
5	Use of privacy-unfriendly default settings	Change the default for some privacy invasive capacities.	Centrally turn off all privacy-invasive other components if not necessary for the performance of the work.
		Change the technical access for applications, limit access to specific components and files based on specific consent from users.	

Conclusions

If government organisations follow the previous recommendations from SLM Rijk to use Windows 10 Enterprise only with the lowest level of telemetry, the Security level (or disable telemetry traffic), and prevent users from syncing their activities via the Windows Timeline, there are no high data protection risks resulting from the diagnostic data collection in Windows 10 Enterprise.

This report identifies contractual, technical and organisational measures Microsoft and the government organisations can take to completely remove the remaining low risks.

On 21 May 2019, Microsoft has released version 1903 for Windows 10 Enterprise. This version enables organisations to use Windows Update for Business functionality when the diagnostic data level is set to Security. In previous versions, this functionality was only available at the telemetry level 'Basic' or higher.

SLM Rijk is providing significant input to Microsoft for an upcoming structural solution for Windows 10 Enterprise customers which is being designed for Windows 10 Enterprise 1809 and later versions. This will allow government organisations to have a simplified compliance solution for Windows 10 Enterprise at diagnostic data levels above Security. This solution will be ready in the foreseeable future, and Microsoft plans to make an announcement about this solution later this year.