Ministerie van Justitie en Veiligheid

Microsoft Intune

Data protection impact assessment Microsoft Intune

Version 1

Date	30 June 2020
Status	Public

Colophon

Commissioned by	**Ministry of Justice and Security** Directie Informatievoorziening en Inkoop Strategic Vendor Management Microsoft, Google, Amazon (SLM Rijk) Turfmarkt 147 2511 DP Den Haag Postbus 20301 2500 EH Den Haag www.rijksoverheid.nl/jenv
Contact	Paul van den Berg T 070 370 79 11 p.j.van.den.berg@minjenv.nl
Attachment	Included: executed test scenarios
Authors	**Privacy Company** www.privacycompany.eu Sjoera Nas and Floor Terra

Contents

Figures

Tables

Summary

This Data Protection Impact Assessment (DPIA) assesses the risks for data subjects (government employees) of the use of Microsoft Intune. Intune is an online management and protection service for all kinds of mobile devices, not only for Windows desktops and laptops, but also for mobile phones and tablets with the macOS, iOS and Android operating system.

Government organisations can use Intune to centrally register personal and corporate mobile devices, and encrypt personal data on the devices. Government organisations can also control through Intune that users are not putting the devices into an unsafe mode, and erase or selectively wipe data in case of device loss.

The DPIA identifies the risks caused by government organisations' own management activities as well as the risks that might be caused by Microsoft due to the Intune service, related to the chosen type of enrolment and level of security. This may involve the processing of data on location, application usage and work patterns.

This DPIA contains outcomes with respect to data processing as a result of the use of Intune as at 16 March 2020. Since then, SLM Rijk and Microsoft agreed upon measures with respect to data protection risks 1 and 4 set out below. The measures are included at the end of this Summary. Once these measures have been implemented by Microsoft, and provided that government administrators take the recommended measures in this DPIA into account, risk 1 will be completely mitigated and risk 4 will be significantly reduced.

Outcome: five low data protection risks
The outcome of this DPIA is that there five low data protection. These low risks are due to the following circumstances:

1. Microsoft acts as a data controller for the Company Portal app
2. System administrators can covertly change the status of the device from personal to corporate: if they do, they can see all installed apps on the device.
3. There is no central opt-out functionality for the collection of telemetry data and debug logs from the app.
4. Microsoft is not transparent about the data processing via the Company Portal app.
5. Microsoft processes in, or transfers personal data to, the USA.

The risks are described in the table below, with suggestions for the measures Microsoft and the government organisations can take to further mitigate these low risks. The assessment that the data protections are low, and not high, is based on the relatively innocent nature of the diagnostic data: no content data or other data of a sensitive nature, nor detailed records of individual behaviour. Additionally, government organisations can take effective measures to prevent the collection of sensitive data from the devices.

Umbrella DPIA versus individual DPIAs
Strategic Vendor Management Microsoft (SLM Rijk), housed within the Dutch Ministry of Justice and Security, procures Microsoft licenses for the 300.000 government officials. SLM Rijk negotiated major privacy improvements with Microsoft between November 2018 and May 2019. However, the individual government organisations buy the licenses and determine the settings and scope

of the processing by Microsoft. Therefore this general DPIA can help the different government organisations with the DPIAs they must conduct, but this document does not replace the specific risk assessments the different government organisations must make. Only government 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.

Microsoft Intune for MAM and for MDM
Government organisations can use Microsoft Intune for two different security purposes, namely (1) controlling the access of apps on the devices to the (personal) data processed by the organisation and (2) enforcing compliance by the devices with the information security policy. These two of management capabilities are hereafter referred to as MAM (Mobile Access Management) and MDM (Mobile Device Management).

Different operating systems
This DPIA describes Intune data processing for users with the following operating systems: Apple iOS, Mac OS X, Android and Windows 10 Enterprise. Other platforms such as Surface Hub, Windows 10 Mobile, Windows Holographic for Business and Windows 8.1 are outside the scope of this DPIA.

Type of enrolment: personal and corporate
This DPIA describes two different ways to enrol devices in Intune: by employees themselves as a personal device or by the system administrators as a corporate device. In both scenario's the devices are *self-managed*, and can also be used for personal use. The choice for the type of Intune enrolment (personal or corporate) is independent of the type of purchase. An organisation may allow employees to buy their own personal devices (Bring Your Own Device) or purchase the devices for their employees (Choose Your Own Device).

Intune offers a third type of enrolment: fully managed or supervised mode. In this type of enrolment, devices are fully managed by the organisation. The devices can only be used for authorised work purposes, and not for personal use. The risks of this third type of enrolment have not been assessed in this DPIA.

Intune logfiles, Company Portal app and Azure AD
This DPIA covers the diagnostic data processing via the Intune cloud service, as well as the data processing via the Intune Company Portal app. Users of self-managed devices must install this app in order to be able to manage their devices via Intune. Only users of Windows 10 Enterprise devices can use a browser to register for Intune. This DPIA also covers the use of the Microsoft Azure Active Directory, as its use is mandatory for both MDM and MAM.

Results of technical research
This DPIA is based on a combination of legal analysis of the improved framework contract from SLM Rijk with Microsoft as well as a technical analysis of the actual data processing via Intune. In order to map the data processing via the Intune cloud service, Privacy Company designed and executed (in September/October 2019) a number of test scripts with representative user actions on the four different platforms. Some of these tests were repeated in March 2020. The network traffic from the app was recorded and the three different Intune log files that Microsoft offers to the administrators were reviewed.

In addition, Microsoft collects data on employee behaviour in the Azure Active Directory log files, such as log-in and log-out times. The use of the Azure AD is

mandatory in order to be able to register devices in Intune, both with MDM and with MAM. Government organisations already collect data about the logging in and out of employees and the devices used for this, in other log files about authentication on the network, without of the use of Intune. However, using the Azure AD makes correlation with other available data easier. Therefore, this processing could pose additional risks to data subjects in combination with the Intune logs. This DPIA therefore also reviews the settings of the Azure AD and the audit logs about its use.

Company Portal app
The technical inspection of the Intune Company Portal app shows that Microsoft collects data in two ways: because it sends telemetry data from the Company Portal app to itself and via an error detection log (debug log) that it creates on this app. Users can choose to send this debug log to Microsoft in the event of an error.

Via the telemetry traffic from the app, Microsoft collects a number of unique identifiers of the device and of the user, identifiers such as the IMEI and the e-mail address, and sends them to its own domain in the U.S. (mobile.pipe.aria.microsoft.com). In doing so, Microsoft does not collect any content data or records of users' actions or activities.

Microsoft does not publish any information about the content of the app's telemetry traffic, and does not make a Data Viewer Tool available to inspect the (decoded) contents of the data. Both in September/October 2019 and in March 2020, Microsoft intercepted the attempts to use a proxy and logged the used mitmproxy certificate. During the first tests, in September/October 2019, only telemetry data from two of the platforms could be inspected, namely iOS and macOS. The telemetry data sent from the Android platform are protected against interception with certificate pinning. Intune telemetry data from the Windows platform could not be analysed because registration does not require use of the separate Company Portal app and the telemetry is part of the general telemetry flow from Windows 10. In the second test run, traffic from macOS was also protected with certificate pinning.

Intune log files
This analysis shows that Microsoft processes a large number of unique identifiers via the Intune log files, but not data of a sensitive nature or detailed records of individual behaviour.

Privacy Company initially registered the devices on the four platforms as ‘personal’ with Intune, and later changed the status to ‘corporate’. The administrators see more information from corporate devices. On corporate iOS, macOS, Android and Windows 10 devices administrators can see all apps installed via the respective app stores, including apps that are not managed by government organisations, such as health related apps. On corporate iOS devices they can also see the (private) phone number of an employee. Users do not receive a warning about the status change. They can only find out if they would open the Company Portal app, and look under the status or under the tab notifications. But after installation, there is no technical need for users to open the app.

Intune offers less management options for personal devices. For example, administrators cannot retrieve the Bitlocker key or KeyVault key for the employee and cannot provide policy updates.

Purposes, roles and legal bases

Thanks to the improved privacy guarantees SLM Rijk negotiated in June 2019 with Microsoft for all online services, Microsoft acts as a data processor for the cloud-part of the Intune services. However, Microsoft considers itself to be an (independent) data controller for the data processing via the Company Portal app. Employees must install this app on their self-managed devices to enrol their device in Intune. When the government organisations enable Microsoft to collect personal data via Intune about the use of the apps, they are de facto joint controllers with Microsoft for the processing of the diagnostic data via the Company Portal apps. As a result, government organisations can be held accountable for the risks that data subjects run with regard to the unlawful processing of their personal data. However, there is no joint controllers contract.

Government organisations cannot rely on the consent of employees for the processing of personal data through registration of devices in Intune. Because of the adverse consequences of a possible refusal, consent cannot be freely given. Therefore neither Microsoft nor government organisations have a legal ground for data processing via the apps for purposes that are not strictly necessary for the (technical) functioning of the apps.

Five low risks and measures

Low risks	Measures government organisations	Measures Microsoft (via SLM Rijk)
Unauthorised access by organisations' system administrators to personal data on personal devices	Explicit prohibition to change the status of devices from personal to corporate without information and prior warnings	Privacy by default: the Company Portal app must always provide an active warning to the user in the event of a change in management status, or actively request consent from data subjects
	Logging & systematic monitoring of the behaviour of system administrators in accordance with specific policy, check measures such as a certificate of conduct (VOG)	
Risk that Intune is perceived as an employee monitoring system: Chilling effect employees	Expand the internal privacy policy with rules for logging and purposes for access	Data minimisation: the default setting at Microsoft is a retention period of one year for the Intune audit log files, while the administrators may only need a shorter retention period. The administrators must be able to determine the period themselves
	Create internal privacy page about Intune and explain what the organisation will and won't do with Intune MDM and MAM and the Azure AD	
	Check the available functionalities and/or use of full device management capabilities against internal privacy policy and authorisation matrix	
Lack of purpose limitation data processing via the	Advise employees to turn off both the telemetry flow and the debug log and put	Act as processor for the Company Portal app: all necessary Intune

Company Portal app	the telemetry level in Windows 10 Enterprise on Basis or Security to minimise data traffic to Microsoft in its role as the controller	processing in accordance with the privacy amendment
		Privacy by default: offer administrators the option to centrally disable telemetry and debug log via the Company Portal app
Lack of transparency diagnostic data Company Portal app	Supplement information from Microsoft on internal privacy page about the types of data with factual findings from this DPIA	Publish information about the nature of the data collected through the Company Portal app and debug log
		Provide data viewer tool to view traffic from the Company Portal app
Transfer of personal diagnostic data to the U.S.	Follow recommendations SLM Rijk following case law of EU Court of Justice	Consider processing of personal data Azure AD exclusively in the EU, in particular MFA
		Data minimisation by allowing administrators to determine retention period Intune log files and to centrally disable telemetry from the Company Portal app

Conclusions
This DPIA concludes that government organisations can deploy Intune for self-managed devices without high data protection risks for the government employees. However, there are five low risks. Two of those risks are related to the mandatory use of the Intune Company Portal app, two other risks are related to the nature of registering information about employees' devices, and the last risk stems from the fact that Intune is a cloud service provided by Microsoft, a U.S.-based provider.

This DPIA recommends 8 measures Microsoft should take. SLM Rijk will continue to negotiate with Microsoft to ensure that Microsoft will only process the data that it collects via the app as a data processor and under no circumstances as the controller.

This DPIA focussed on self-managed devices, either as personal or corporate devices. The actual risks depend on the factual implementation per organisation. An organisation can also use Intune to manage corporate devices in fully supervised mode. This type of enrolment allows for greater access to user activities and behaviour. Each government organisation should therefore conduct its own DPIA, based on this umbrella DPIA, to determine what measures are necessary to enforce compliance with its information security policy, without causing high data protection risks for the government employees.

Other measures government organisations can take to mitigate the low risks are:

1. Advise employees to turn off telemetry and debug logs in the Company Portal app

2. Add an explicit policy rule to the existing internal privacy policy that administrators may not change the status without informing and alerting the user
3. Systematically check the log files about the administrators' behaviour, in accordance with existing policies
4. Ensure administrators have a valid certificate of conduct.
5. Expand the internal privacy information with an explanation of the purposes and categories of data collected through Intune MDM and MAM, what the system administrators can and cannot see on the self-managed devices.

Measures Microsoft
This DPIA was conducted between September 2019 and March 2020 and contains outcomes with respect to processing in connection with the use of Microsoft Intune as at 31 March 2020. SLM Rijk provided Microsoft with the DPIA findings upon completion of this DPIA. Between April and June 2020, SLM Rijk and Microsoft agreed upon measures to mitigate two of the five low data protection risks ultimately in the fall of 2020. These measures are:

1. Microsoft will only act as data processor for the Intune Company Portal App, with the exception of processing for Microsoft's own legitimate business purposes, and all processing will be in accordance with the privacy amendment.

2. Microsoft will publish documentation about the nature of the data collected through the Company Portal App and debug logs. This documentation must provide customers with a good understanding of the data that Microsoft collects.

These measures will have to be implemented at the latest in the fall of 2020. SLM Rijk will publish an update about the implementation progress early 2021.

Introduction

DPIA: what is it and why is it mandatory?
Under the terms of the General Data Protection Regulation (GDPR), an organisation may be obliged to carry out a Data Protection Impact Assessment (DPIA) under certain circumstances, for instance where large-scale processing of personal data takes place. The assessment is intended to shed light on, among other things, the specific data processing activities, the inherent risk to data subjects, and the safeguards applied to mitigate these risks. The purpose of a DPIA is to ensure that any risks attached to the process in question are mapped and assessed, and that adequate safeguards have been implemented to tackle those risks.

A DPIA was previously also referred to as PIA, privacy impact assessment. According to the GDPR, a DPIA is about the risks to the rights and freedoms of natural persons. Data subjects have a fundamental right to the protection of their personal data and a number of other fundamental *freedoms* that may be affected by the processing of personal data. The right to data protection is therefore a broader right than just the right to privacy. Consideration 4 of the GDPR states: "*This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity*". Nevertheless, for the sake of readability, this report sometimes uses the term 'privacy risk' to refer to these risks to the rights and freedoms of data subjects, and not the legally correct term 'data protection risk'.

Pursuant to Article 35 of the General Data Protection Regulation (GDPR), a DPIA is mandatory if an intended data processing constitutes a high risk for the data subjects whose personal data are being processed. The Dutch Data Protection Authority (Dutch DPA) published a list of 16 types of processing for which a DPIA is always mandatory in the Netherlands.[1] If a processing is not included in this list, an organisation must itself assess whether the data processing is likely to present a high risk. The European national supervisory authorities (hereinafter referred to as the Data Protection Authorities or DPAs), united in the European Committee also published a list of 9 criteria.[2] As a rule of thumb, if a data processing meets 2 of these criteria, a DPIA is required.

Microsoft Intune is an online management and protection service for all kinds of mobile devices, not only for Windows desktops and laptops, but also for mobile phones and tablets with the macOS, iOS and Android operating system.

Government organisations can use Intune to centrally register personal and corporate mobile devices, and encrypt personal data on the devices. Government organisations can also control through Intune that users are not putting the

[1] Dutch Data Protection Authority, Data protection impact assessment (DPIA), URL: https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667
[2] See WP248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

devices into an unsafe mode, and erase or selectively wipe data in case of device loss.

It is likely that Microsoft and government organisations will process personal data about the behaviour of employees and system administrators through the use of Intune. In Intune's chosen set-up, Microsoft and/or government organisations do not process any data about other data subjects, for example via the content of communications or files.

Government organisations are obliged to carry out a DPIA for these processing operations, because the data processing meets two, and perhaps three, of the nine criteria set by the European Committee. The criteria are:

- Possibility that these processing operations (via the Intune log files) lead to a systematic observation of the behaviour of employees (criterion 3);
- Data relating to vulnerable data subjects (criterion 7, employees are in an unequal relationship of power with employers);
- Large scale processing of data (criterion 5, the processing can affect over 10,000 employees[3]).

Apart from that, in the opinion on data processing in the workplace, the DPAs write that organisations always have to do a DPIA before using MDM technology:

"*A DPIA should be performed prior to the deployment of any such technology where it is new, or new to the data controller. If the outcome of the DPIA is that the MDM technology is necessary in specific circumstances, an assessment should still be made as to whether the resulting data processing complies with the principles of proportionality and subsidiarity.*"[4]

The Dutch DPA mentions two other specific criteria when the performance of a DPIA is mandatory:

- Location data (criterion 12). Large-scale processing and/or systematic monitoring of location data from or traceable to natural persons. For example, by (..) telephones (..);
- Communication data (criterion 13). Large-scale processing and/or systematic monitoring of communication data including metadata traceable to natural persons, unless and insofar as this is necessary to protect the integrity and security of the network and the service of the provider involved or the end user's peripheral device.[5]

It is possible that the DPIA shows that there is no systematic monitoring of location data, or that the monitoring of communication data is necessary to protect the integrity and security of the network. However, in order to be able to assess the

[3] Neither the European nor the Dutch regulators use a fixed number for the 'large-scale' criterion. Nevertheless, the Dutch Data Protection Authority (Dutch DPA) has indicated that the processing by healthcare providers other than hospitals, GPs' surgeries and healthcare groups is large-scale if they process data of more than 10,000 patients in a single information system. Dutch DPA, Explanation of the term 'large-scale' clarified for all healthcare providers, 11 December 2018, URL: https://autoriteitpersoonsgegevens.nl/nl/nieuws/uitleg-begrip-%E2%80%98grootschalig%E2%80%99-verduidelijkt-voor-alle-zorgaanbieders

[4] Article 29 Working Party, WP 249, opinion 2/2017 on data processing at work, 8 June 2017, URL: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=54650, p. 20.

[5] Dutch DPA, Data protection impact assessment (DPIA), URL: https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667

impact of the data processing and to determine whether the actual processing meets the requirement of necessity, government organisations must first carry out a DPIA (or have it carried out). This DPIA compares the opportunities with the risks and assesses whether measures are possible and necessary to mitigate any risks.
This DPIA follows the structure of the DPIA Model mandatory for all Dutch government organisations.[6]

Umbrella DPIA versus individual DPIAs
Microsoft's Office 365 software is used by approximately 300.000 employees and workers in the Dutch ministries, parliament, the High Councils of state, the advisory commissions, the police, the fire department and the judiciary, as well as the independent administrative authorities. As Intune is included in most Enterprise licenses[7] it is plausible that many government organisations are already using, or considering the use of Intune.

In GDPR terms SLM Rijk is not the data controller for the processing of diagnostic data via the use of the Office software. However, as central negotiator with Microsoft, it has a moral responsibility to assess the data protection risks for the employees and negotiate for a framework contract that complies with the GDPR. Therefore, SLM Rijk commissions umbrella DPIAs to assist the government organisations to select a privacy-compliant deployment, and conduct their own DPIAs where necessary. Only government organisations themselves can assess the specific data protection risks, related to the technical privacy settings, nature and volume of the personal data they process and vulnerability of the data subjects.

This umbrella DPIA is meant to help the different government organisations with the DPIA they must conduct, but this document cannot replace the specific risk assessments the different government organisations must make.

Previously published DPIAs SLM Rijk
In October 2018 SLM Rijk published a DPIA report about Office 365 ProPlus, version 1708 and Office 2016. The report was published on the Dutch government website with an update on the negotiations between the Dutch central government and Microsoft about the GDPR compliance.[8]

In May 2019, SLM Rijk concluded the negotiations with a privacy-improved contract with Microsoft for the online services. Simultaneously, Microsoft released new Enterprise versions of Office 365 and Windows 10 with many of the required technical improvements to lower data protection risks for the end-users.

[6] *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017). For an explanation and examples (in Dutch) see: https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia.
[7] Microsoft provides a list of licenses that include the use of Intune at https://docs.microsoft.com/en-us/intune/fundamentals/licenses: Microsoft 365 E5, Microsoft 365 E3, Enterprise Mobility + Security E5, Enterprise Mobility + Security E3, Microsoft 365 Business, Microsoft 365 F1, Microsoft 365 Government G5 and Microsoft 365 Government G3. Additionally, Intune for Education is included in Microsoft 365 Education A5 and Microsoft 365 Education A3.
[8] SLM Rijk, URL: https://www.rijksoverheid.nl/documenten/publicaties/2018/11/12/strategisch-leveranciersmanagement-microsoft-rijk-slm-microsoft

In July 2019, SLM Rijk published three new DPIA reports about the new versions of Microsoft Office 365 ProPlus, Office Online and the mobile Office apps and Windows 10 Enterprise, versions 1809 and 1903.[9]
The role of SLM Rijk is not limited to Microsoft Office. As representative of all the procuring government organisations, SLM Rijk assesses the risks for all Microsoft products and services that are commonly used by government organisations, such as Windows, Office, Dynamics and Azure and approaches the risk mitigating measures with a holistic view. Microsoft has been working constructively with SLM Rijk during the review of the risks of the use of these products.
In the volume licensing contracts, Microsoft releases new versions of its Office 365 ProPlus and Windows Enterprise software twice per year. As part of its ongoing commitment to ensure GDPR compliance, SLM Rijk intends to regularly commission new DPIAs on new versions of Windows 10 and Office 365, to guarantee the rights of data subjects on ongoing basis. New DPIA's can be necessary to examine the risks of changes in the technology and processing methods, to take account of modifications of the applicable laws and/or relevant jurisprudence, and to assess changes in the contractual framework with Microsoft.

SLM Rijk also commissioned DPIAs on the data processing risks of using Microsoft's Azure cloud services and Microsoft Dynamics. SLM Rijk is expanding its vendor management role to other providers of cloud services, and also commissioned DPIA report on the use of Google G Suite and Amazon web and database services. These DPIAs are work in progress.

The DPIA reports have been written by the Dutch privacy consultancy firm Privacy Company.[10]

Technical research
In order to map the data processing via Intune, a number of test scripts were developed that contain a selection of representative user actions on the various end-user devices. On each of the four platforms Office 365 was installed, licensed by an anonymous tenant. In September/October 2020 version 1909 was tested. In March 2020, the monthly channel version 2001 was tested. The (different) devices were centrally registered in the organisation's Intune test environment. Initially, in September/October 2019, the test scripts were performed manually on each of the four test platforms. During the retest in March 2020, on a Microsoft 365 Business Premium license, limited scenarios were executed. The retests were focussed on the telemetry from the Company Portal app.

Inspections conducted per device

System and OS September/October 2019	System and OS March 2020
iPhone X with iOS 12.4	iPhone XS Max with iOS 13.3.1[11]
Google Pixel with Android 9	Google Pixel 3 XL with Android version 10 build QQ1A.200205.002[12]
Dell laptop with Windows 10 Enterprise version 10.0.18362.30.19h1_release	Dell Latitude Windows 10 Enterprise 1803, build 17134.1304

[9] All DPIA reports are published in English, with a summary in Dutch. See the overview on the website of SLM Rijk), URL: https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise
[10] https://www.privacycompany.eu/ At the request of SLM Rijk, Privacy Company has summarised the results in English and Dutch blogs, for example: https://www.privacycompany.eu/blogpost-en/microsoft-improves-privacy-terms-for-office-for-all-organisations
[11] Company Portal for iOS version 4.3.1.
[12] Company Portal for Android version 5.0.4700.0.

Macbook with macOS 10.14.6	Macbook with macOS 10.15.3

In both tests, the network traffic was recorded to the extent technically possible. A TLS-termination proxy was used, but due to certificate pinning, sometimes no traffic was sent. Compared to the September/October tests, Microsoft added certificate pinning to the MacOS Company Portal app. Therefore, in March 2020, only the telemetry traffic from the iOS app could be intercepted. In addition, a copy was made of the Intune application's log data (generated during the tests).

The audit logs of Intune and the Azure AD were inspected and a digital request was made to Microsoft (Data Subject Request), as referred to in article 15 of the GDPR, to export all personal data related to both test accounts. No separate data subject access request was sent to Microsoft as a data controller for access to the personal data collected via the app, due to time constraints. This analysis is based on the logs and the intercepted telemetry traffic.

Structure of the DPIA

This assessment follows the structure of the Dutch government *Model Data Protection Impact Assessment (PIA)*.[13] This model consists of the following four parts:

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

Part A describes the (technical) data processing by Microsoft Intune. This covers the types of personal data, the categories of data subjects, processing purposes, roles of the parties involved, interests in the processing, locations where the data are processed, applicable law(s) and the retention periods.

Part B describes and assesses the principles, necessity, proportionality and compatibility of the intended processing in relation to the processing purposes. The proportionality is assessed by conformity with the key data protection principles listed in Article 5 of the GDPR, such as transparency, adequate security, privacy by design and purpose limitation. This section also assesses the lawfulness of transfers of personal data to countries outside of the EEA, and the way in which the rights of data subjects are respected.

Part C describes and assesses the risks to the rights and freedoms of data subjects resulting from the processing of their personal data via Microsoft Intune.

Part D assesses the technical and organisational measures that Microsoft, SLM Rijk or government organisations should take to reduce or eliminate the identified remaining privacy risks, as well as their impact. Finally, this section describes whether there is a residual risk from data processing after the application of the recommend risk mitigating measures.

[13] *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017)., https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia

Part A. Description of the Intune data processing

The first part of this DPIA report describes the characteristics of the data processing via Microsoft Intune. and the roles, processing purposes and interests of government organisations. This section continues with a description of the personal data that may be processed in through the different log files and the Company Portal app, the categories of data subjects that may be affected by the processing, the locations where the data may be stored, processed and analysed, the purposes of the data processing as provided by Microsoft and the roles of the government organisations and Microsoft as processor and data controller. This section also provides an overview of the different interests related to this processing, and of the retention periods.

1. The processing of personal data through the use of Microsoft Intune

Microsoft Intune is an online management and protection service for all kinds of mobile devices, not only for Windows desktops and laptops, but also for mobile phones and tablets with the iOS and Android operating system. Intune is part of Microsoft's online service within Azure, and is linked to the Azure Active Directory authentication service. The use of Intune is included in Microsoft 365 volume licensing licenses.[14]

Microsoft's Office 365 software is used by approximately 300.000 employees and workers in the Dutch ministries, parliament, the High Councils of state, the advisory commissions, the police, the fire department and the judiciary, as well as the independent administrative authorities. As explained in more detail in the introduction to this DPIA, this report assesses the risks of management self-managed devices in Intune, registered as personal or as corporate devices (not the fully managed devices).

With Intune, government organisations can register all self-managed devices and ensure that all data on these devices are encrypted. On Windows 10, Intune can control encryption with BitLocker, on MacOS with FileVault, and on Android and iOS devices with the Company Portal app. Intune allows system administrators to check and prevent that end-users are putting the devices into an unsafe mode. Administrators can also erase all, or selectively wipe some data from the devices in case of loss of devices.

This DPIA identifies the risks caused by government organisations' own management activities in Intune as well as the risks that might be caused by Microsoft due to the logging of activities in the Intune service, related to the

[14] See the graphic Microsoft made itself, of the relation between Intune, Azure AD and the mobile devices of users at, URL: https://docs.microsoft.com/en-us/intune/media/intunearchitecture.svg Deloitte, the SOC auditor for core online services based on Azure, describes Intune as follows: *"Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud. Using Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure."* Microsoft Corporation, Microsoft Azure (Azure & Azure Government), SOC 3 Report, July 1, 2018 - June 30, 2019, p. 33.

chosen type of enrolment and level of security. This may involve the processing of data on location, application usage and work patterns.

1.1 Scope of this DPIA

Intune has two distinct functionalities: Mobile Device Management (MDM) and Mobile Application Management (MAM). This DPIA assesses two different ways to enrol devices in Intune MDM and MAM: by employees themselves as a personal device or by the system administrators as a corporate device. In both scenario's the devices are *self-managed*, and can be used for personal use. Since the use of the Azure Active Directory authentication service is mandatory for this use of Intune MDM and MAM, this DPIA also examines the (additional) risks of the correlation of data from Intune with data from the Azure AD log files.

This DPIA describes Intune data processing for users with the following four operating systems: Apple iOS, Mac OS X, Android and Windows 10 Enterprise. These four platforms have been chosen because they are expected to be the most widely used. For this DPIA, the data processing was tested on each of these four platforms.

Intune logfiles and Company Portal app

This study covers the diagnostic data processing via the Intune cloud service, as well as the data processing via the Intune Company Portal app. Users of self-managed devices must install this app in order to be able to manage their devices via Intune. Only users of Windows 10 Enterprise devices can use a browser to register for Intune (and use the in-built Intune functionality in Windows).

Outside the scope of this DPIA

This DPIA does not analyse the use of Intune on other platforms such as Surface Hub, Windows 10 Mobile, Windows Holographic for Business and Windows 8.1.

Intune can be used to take over the management of devices completely (fully managed or supervised mode). This type of enrolment is only possible via auto enrolment (DEP).[15] In this type of enrolment, the devices can only be used for authorised work purposes, and not for personal use. This enrolment occurs when selected suppliers do the registration of the device in Intune themselves (the manufacturer or distributor of a Macbook, Dell laptop or tablet, or other suppliers of laptops or tablets). With this type of enrolment, devices are automatically registered in the supervised mode (fully managed), and are immediately provided with the necessary encryption.

On such supervised or fully managed devices, it is possible to track the location of the iOS devices running on iOS version 9.3 or later. Administrators can see the location data of a lost or stolen iPhone for up to 24 hours when they turn on the 'locate device' function.[16] This processing is only possible for a fully managed device that can be set to "Lost mode" by the system administrators.[17]

[15] The Device Enrollment Program (DEP) is renamed by Microsoft to "Automated Device Enrollment". All devices enrolled via ADE, are automatically enrolled in supervised mode. Source: blog Robin Hobo, 30 September 2019, URL: https://www.robinhobo.com/how-to-enroll-an-apple-device-with-ios-13-user-enrollment-mode-in-microsoft-intune/

[16] https://docs.microsoft.com/en-us/intune/remote-actions/device-locate

[17] Microsoft, Enable lost mode on iOS devices with Intune, 25 April 2018, URL: https://docs.microsoft.com/en-us/intune/remote-actions/device-lost-mode Microsoft writes: "*To use lost mode, the device must be a corporate-owned iOS device that is in supervised mode.*"

Organisations that want to fully manage desktops and laptops and only allow the use of Windows 10 Enterprise can also for example use Microsoft's on-premises Mobile Device Management through the Microsoft Endpoint Manager (previously named System Center Configuration Manager, SSCM). These functionalities to fully manage the end-user equipment fall outside of the scope of this DPIA. However, the risk is addressed that an administrator can change the status of a device in Intune MDM, from personal to corporate.

It is possible to apply Intune MAM to devices that are not registered in Intune. For example, on employees' own mobile devices (Bring Your Own Device). This DPIA does not deal with the risks of data processing via Intune MAM for apps without registration in Intune (APP WE, Without Enrollment).

By using Intune MAM, government organisations can manage four types of apps: (1) Microsoft's own Office apps, (2) Microsoft partner apps, (3) third-party apps, and (4) self-developed apps. Commonly used partner apps that can be managed with Intune include Adobe Acrobat Reader for PDF files, Citrix Secure Mail and Sharefile, and iBabs for meeting scheduling. Administrators can also add existing apps and self-developed apps (Line-Of-Business, LOB-apps).[18] Only the first category of Microsoft Office apps falls within the scope of this DPIA.

Intune MAM offers many detailed *data loss prevention* management options, such as preventing employees from exporting data from Microsoft Office applications to other applications. This includes functions such as copying, pasting and saving documents under a new name at a different location (saving as). With Intune it is also technically possible to force employees to open hyperlinks only with an Intune secured browser.[19]It is possible to use Intune to enforce conditional access per app. But these processing operations fall outside the scope of this DPIA. This report does advise government organisations to be transparent about the chosen type of Intune deployment and to take other internal measures to prevent that these technical possibilities culminate in a *chilling effect* on employees.

With Intune MAM, government organisations can also choose to only give access to a limited version of the app stores (managed app store). They could also assign and track apps purchased through a volume purchasing program via the Microsoft app store. For example, government organisations could enable a license for a specific work tool, such as a calculation module. This processing falls outside the scope of this report, but should be considered by the individual organisations that wish to deploy Intune in a privacy friendly way.

Finally, the risks of any future use of *mobile threat defence,* whereby Microsoft or external suppliers can process personal data for mobile virus/malware detection and clean-up, fall outside the scope.[20] It is up to the individual government organisations to take stock of the privacy and security risks, and to assess what

[18] Microsoft explains: "*A line-of-business (LOB) app is an app that you add to Intune from an app installation file. This kind of app is typically written in-house. Intune installs the LOB app on the user's device.*" Microsoft, Add an Android line-of-business app to Microsoft Intune, 22 August 2019, URL: https://docs.microsoft.com/en-us/intune/apps/lob-apps-android. Also: https://docs.microsoft.com/en-us/intune/apps/lob-apps-ios ans https://docs.microsoft.com/en-us/intune/apps/lob-apps-macos

[19] In the investigated MAM-configuration the option: "*managedBrowserToOpenLinksRequired*" is set to *false*, which means: off.

[20] See, URL: https://docs.microsoft.com/en-us/intune/protect/advanced-threat-protection. Popular applications are: Lookout for work, Symantec, Sandblast en Zimperium. See, URL: https://docs.microsoft.com/en-gb/intune-user-help/you-are-prompted-to-install-lookout-for-work-ios

type of solution best addresses their needs, without creating high data protection risks for the end-users.

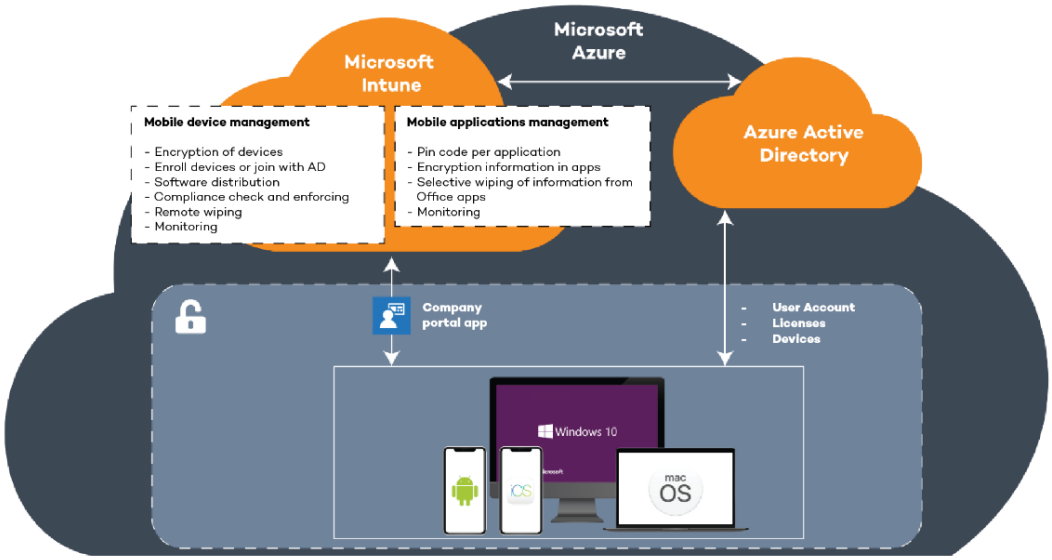
1.2 Intune MDM, Intune MAM and Company Portal app

Government organisation can use Intune to secure the (personal) data on employees' devices in two different ways. The two different security purposes are:

(1) enforce compliance of the devices with the information security policy (MDM)
(2) control access to (personal) data via Microsoft 365 apps on the self-managed devices (MAM)

These two different Intune management options are hereafter referred to as MDM (Mobile Device Management) and MAM (Mobile Access Management).

Figure 1: Intune deployment



1.2.1 *Processing via Intune MDM*

With Intune MDM, organisations can ensure that all employees' self-managed devices comply with the information security policy. Processing via MDM consists of the following components:

- Central registration of all mobile devices;
- Delete [obsolete/disused] mobile devices from the registration, without deleting the data from the device;
- Encrypt mobile phones, tablets and laptops with Bitlocker, Key vault or via the Company Portal app;
- Execute a password policy and determine the minimum number of characters, validity period, and a maximum number of minutes before the screen lock is triggered;
- Distribute software, such as antivirus software;
- Compliance check, if a device has been lost or an employee leaves the organisation, the administrators want to be able to set the status of the device to 'unsafe';
- Remote lock: the ability to remotely encrypt data on the device, provided that the device can be reached. This may be necessary if an employee disables the encryption. Anyone with the correct PIN or access code can decrypt the device again;

- Remove passcode: allows administrators to delete the device's access code so anyone with physical access to the device can access the apps and data on the device;
- Bypass activation lock: bypassing a previous user's access code on iOS devices to be able to give the device to a new user;
- Remote wiping: with user approval, administrators can reset the device to default settings. This will permanently erase all data unless the users have a backup. Except in the case of an emergency, the administrators of government organisations will first seek the user's approval;
- Monitoring.

There are differences in the management options between personal and corporate devices. For personal devices, it is not possible for administrators to show the Bitlocker or Key vault key to the user if the user has forgotten it. Additionally, administrators cannot perform policy updates on personal devices.

1.2.2 Processing via Intune MAM

With Intune MAM, organisations can restrict the access to organisation (personal) data via apps on the self-managed devices that can also be owned by employees (Bring Your Own Device). MAM and MDM can also be used separately, to manage apps on devices that are not registered with Intune via MDM. This is called MAM-WE (Without Enrollment), but this type of Intune use was not inspected for this DPIA.

In this DPIA, the processing via MAM comes on top of the processing via MDM. Government organisations can use Intune MAM for the following purposes:.

- Complement the multifactor authentication (MFA) policy by requiring a PIN code for each application. These measures prevent third parties from logging in on the basis of the *cached credentials* if a device is lost or contaminated with malware;
- Encrypt information in the applications;
- Selectively wipe organisational (personal) data, for example all information from Office apps (instead of erasing all data on the device);
- Aggregated analytics/monitoring, for example which OS versions are used.

Microsoft publishes a list of its own apps and supported apps that can be managed through Intune MAM.[21] Currently, the Microsoft supported apps are: Dynamics (CRM and Field Worker); Azure Information Protection Viewer, Bookings, Cortana, Edge, Excel, Power Automate, Intune Managed Browser, Invoicing, Kaizala, Launcher, Office (includes Word, Excel and PowerPoint), OneDrive, OneNote, Outlook, Planner, PowerApps, PowerBI, PowerPoint, SharePoint, To-Do, Skype for Business, StaffHub, Stream, Teams, Visio Viewer, Word, Work Folders and Yammer. Beside the four purposes mentioned above, administrators can set various restrictions to these apps, such as preventing the copying, pasting, and saving of documents under a different name. As explained in the introduction of this report, under the heading 'Outside the scope of this DPIA', the risks of such restrictions are not assessed in this report.

Figure 2 illustrates what apps were used during the tests with Intune MAM on iOS and Android. These were: Excel, Outlook, Powerpoint, Word, Onenote, Planner, PowerBI, Sharepoint, SkyDrive, Teams (including Skype functionality on iOS),

[21] Microsoft, Microsoft Intune protected apps, 25 February 2020, URL: https://docs.microsoft.com/en-us/intune/apps/apps-supported-intune-apps

Edge (on Android), PowerApps (on Android), Skype for Business (on Android), Microsoft Stream (on Android), To-do's (on Android) and StaffHub (on Android). For the apps on macOS and Windows, no rules were set via Intune MAM.

Because Microsoft has less control over devices with an operating system other than Windows, application management via Intune MAM works differently on devices with Android or iOS as operating system. On Windows and MacOS, it is technically impossible to ensure that data from managed apps is not shared with unmanaged apps. This is possible on Android and iOS.

Figure 2: Management of different apps on iOS and Android

System administrators can use different methods to enrol Intune. Microsoft provides an overview for the four main platforms.[22] The key difference is whether the device is registered as personal device (Bring Your Own, Choose Your Own) or as corporate device (purchased by the organisation).

On Windows, if Intune is used by domain join (via the Azure AD), the device will automatically be registered as corporate. On the other three platforms, administrators can register the devices for the users if they enter the serial number of the device in Intune. If this is not the case, the user must register himself. The device will then be registered as personal.

The actual differences in the types of data processed per platform, in the app, via Intune MDM and via Intune MAM are described in Sections 2.2 (*Three types of Intune log files*) and 2.3 (*Data processed by Microsoft through the Company Portal app*) of this report: the findings of the technical research into the diagnostic data.

[22] Microsoft, What is device enrollment? 24 April 2019, URL: https://docs.microsoft.com/en-us/intune/enrollment/device-enrollment

Section 2.4 describes the data that Microsoft additionally processes via the Azure AD.

Table 1: Overview of app management capabilities per platform relevant to government organisations[23]

Management options apps/operating system	Android	iOS	macOS	Windows 10
Adding and assigning apps to devices and users (antivirus software)	Yes	Yes	Yes	Yes
Use policy to set up mobile Office apps to renew expired apps	No	Yes	No	No
Store company data in Office apps only within Office365[24]	Yes	Yes	No	No[25]
Only delete business data from an installed app (selective deletion app)	Yes	Yes	No[26]	Yes
Checking app allocations[27]	Yes	Yes	Yes	Yes
Obligatory installation of apps on devices (required)[28]	Yes	Yes	Yes	Yes
Updating Office Apps	Yes	Yes	No	Yes

1.2.3 *Microsoft Intune Company Portal app*

To gain secured access to the data in the applications managed with Intune MAM and MDM, all employees that use self-managed devices must first install a free app, the Microsoft Intune Company Portal app. Only on devices running Windows 10 it is possible to register at Intune via a browser, without installing the separate app.

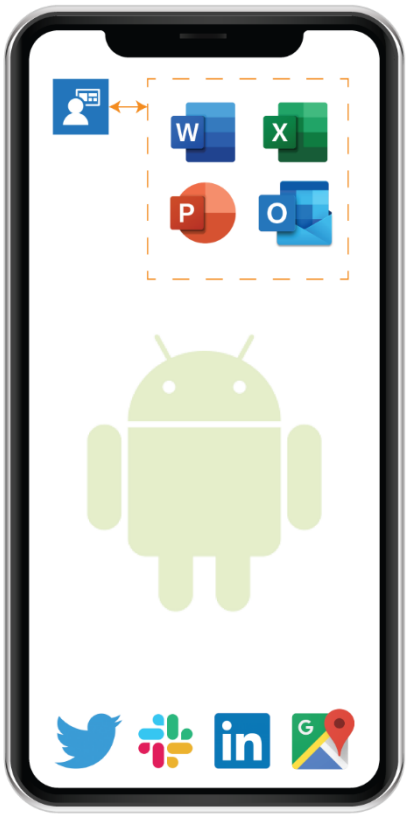
There is a difference in the way the app works with Intune MAM and with Intune MDM. If government organisations would like to roll out Intune MAM without registering with Intune MDM (MAM-WE, Without Enrollment), the user still has to install the app on Android, but the user will not have to log in with his account.[29] On iOS, applications can only be managed through Intune without enrollment if the developer of the app used the Intune software development kit, like, for example, the iOS apps for Microsoft Office.[30]

[23] Microsoft, What is Microsoft Intune app management?, 27 February 2020, URL: https://docs.microsoft.com/en-gb/intune/apps/app-management
[24] In the tested MAM configuration copy/paste restrictions on iOS en Android were turned Off. There was only a policy for the storage location of data. The policy "allowedDataStorageLocations" allowed the following two options: "oneDriveForBusiness" and "sharePoint".
[25] Microsoft recommends to use Windows Information Protection to protect apps on devices that run Windows 10. See footnote 1 in Microsofts explanation quoted in the footnote 22.
[26] As there is no selective wiping option in Intune for macOS, system administrators can only wipe the entire macOS. It has been checked that this is indeed the case when a wiping instruction is given. The device then needs a full reinstall of the operating system.
[27] The tests shows the permissions are generic, to have or not have access to Intune.
[28] This option is relevant when a government organisation wants to distribute antivirus software.
[29] Microsoft, Frequently asked questions about MAM and app protection, URL: https://docs.microsoft.com/en-us/mem/intune/apps/mam-faq *Why is the Company Portal app needed for Intune app protection to work on Android devices?*
[30] Microsoft, Microsoft Intune App SDK for iOS developer guide, 2 January 2020, URL: https://docs.microsoft.com/en-us/mem/intune/developer/app-sdk-ios It appears the Company Portal app is always required on macOS for Intune MAM (without enrollment is not possible). See for example: https://docs.microsoft.com/en-

The installation of the Company Portal app is slightly different for each OS. Below, the steps are explained with screenshots for Android, iOS, macOS and Windows.

Android
With Intune, Android devices can be managed in two ways: on a per application basis or with a strict separation on the device between the personal environment and the work environment. This DPIA examines the first option, enforcing some specific rules on specific Office365 apps.

Figure 3: Android per-application management



This DPIA examines enrolment with an Android work profile.

Setting up a Work Profile is possible on devices with Android operating system version 5.1, launched end of 2014. As of this version, the operating system has certain management features called Android Enterprise.[31]

After logging into the Company Portal app, employees with an Android device will see a screen with questions about government organisations' Access Setup. This screen explains that their device needs to be managed and that employees need to set up an access code to encrypt the device.

Employees will then see a screen which explains the various authorisations that Intune requests to access data and sensors from the device. Microsoft explains that this is also a generic screen, in which all possible consents are described from the Android operating system, even if government organisations do not need all these authorisations for a long time.[32]

---

us/mem/intune/apps/troubleshoot-mam The possibility of MAM-WE on macOS devices is not mentioned.

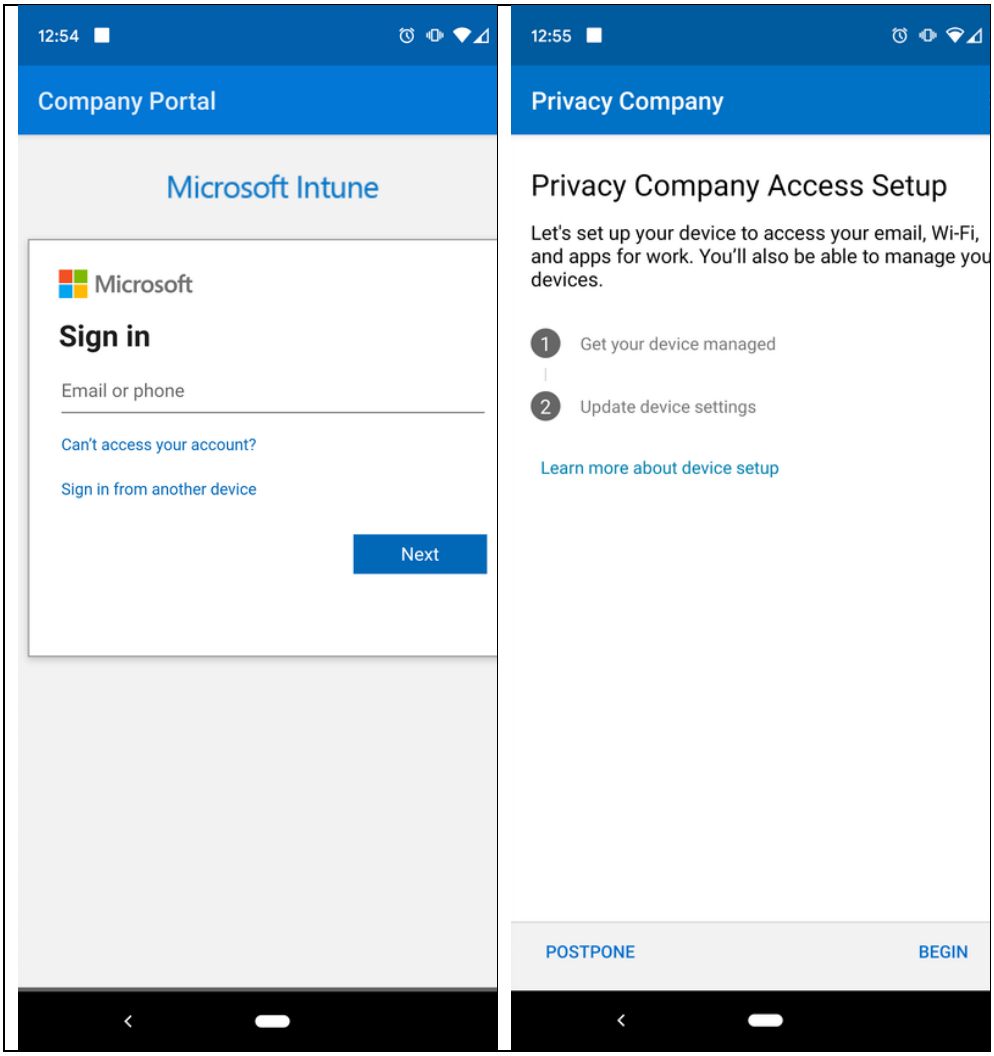
[31] With the introduction of Android Enterprise, Google has implemented „Work Profile", which can be rolled out for BYOD and company-owned devices. It ensures that business and personal data and applications are separated from each other and professional applications and data are stored in a container. URL: https://emea.mobi/ios-13-and-android-enterprise-simplify-the-use-of-byod-devices/ See also Microsofts explanation: "*Devices must meet these requirements to be managed as an Android Enterprise dedicated device:*

- Android OS version 5.1 and above.
- "Devices must run a distribution of Android that has Google Mobile Services (GMS) connectivity. Devices must have GMS available and must be able to connect to GMS." URL: https://docs.microsoft.com/en-gb/intune/enrollment/android-kiosk-enroll

[32] Microsoft, Enrol your device with Company Portal, 31 October 2019, URL: https://docs.microsoft.com/en-gb/intune-user-help/enroll-device-android-company-portal. Microsoft writes: "*Microsoft does not control the messaging on this screen. We understand that its phrasing can seem somewhat drastic. Company Portal can't specify which restrictions and access are relevant to your organization. If you have questions about how*

There is also a separate Microsoft Intune app for Android devices. This app is aimed at organisation owned devices and is less suitable for Bring Your Own Devices.[33]

Figures 4 and 5: Logging in into the Company Portal app and organisation Access Setup with Android

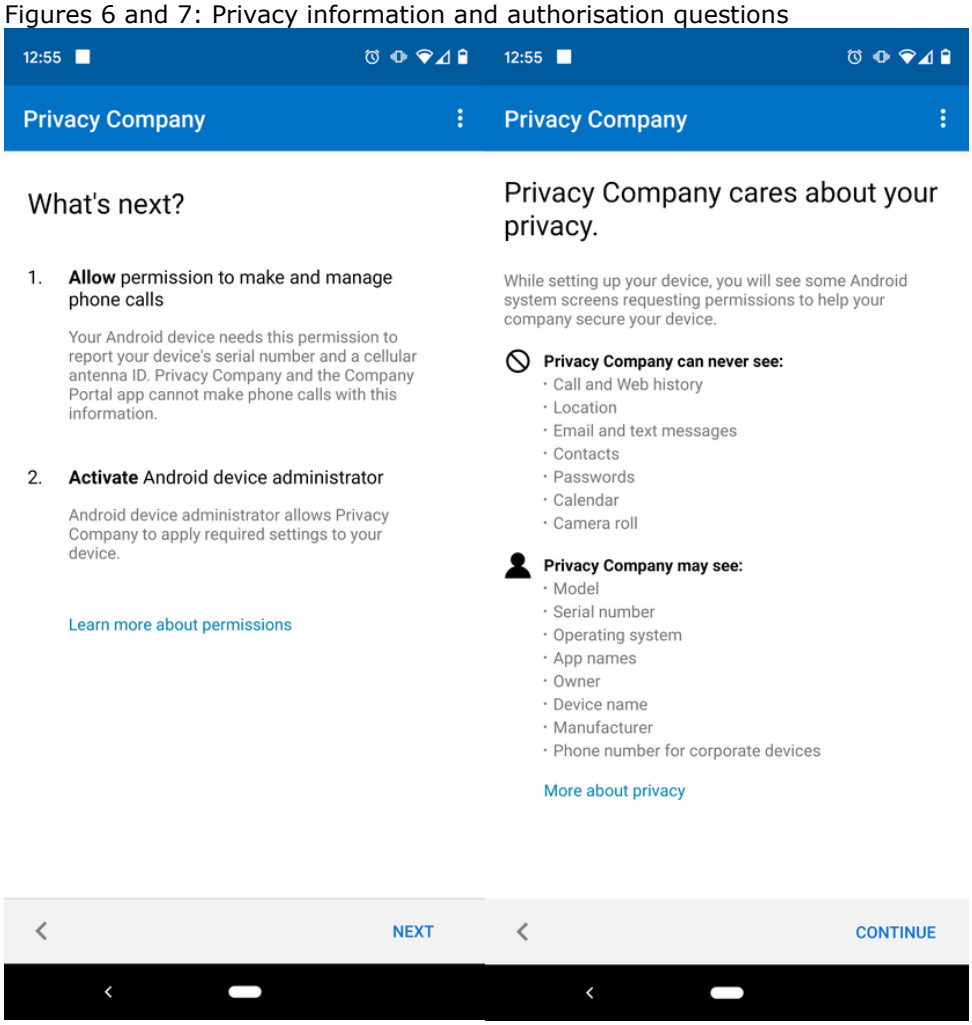


In the next screen (Figure 6) the app shows what the organisation can and cannot see through the app. If an employee clicks on the 'More about privacy' link [circle added for clarity], he or she should ideally be directed to an internal website of the organisation with specific privacy information, for example a FAQ with a section explaining what the organisation can and cannot see about user behaviour on the device / in the apps.

your organization uses the app, contact your IT support person. Go to the Company Portal website to find your organization's contact information."

[33] Microsoft, Enrol you corporate device with the Microsoft Intune app, 8 July 2019, URL: https://docs.microsoft.com/en-gb/intune-user-help/enroll-device-android-microsoft-intune-app

Figures 6 and 7: Privacy information and authorisation questions

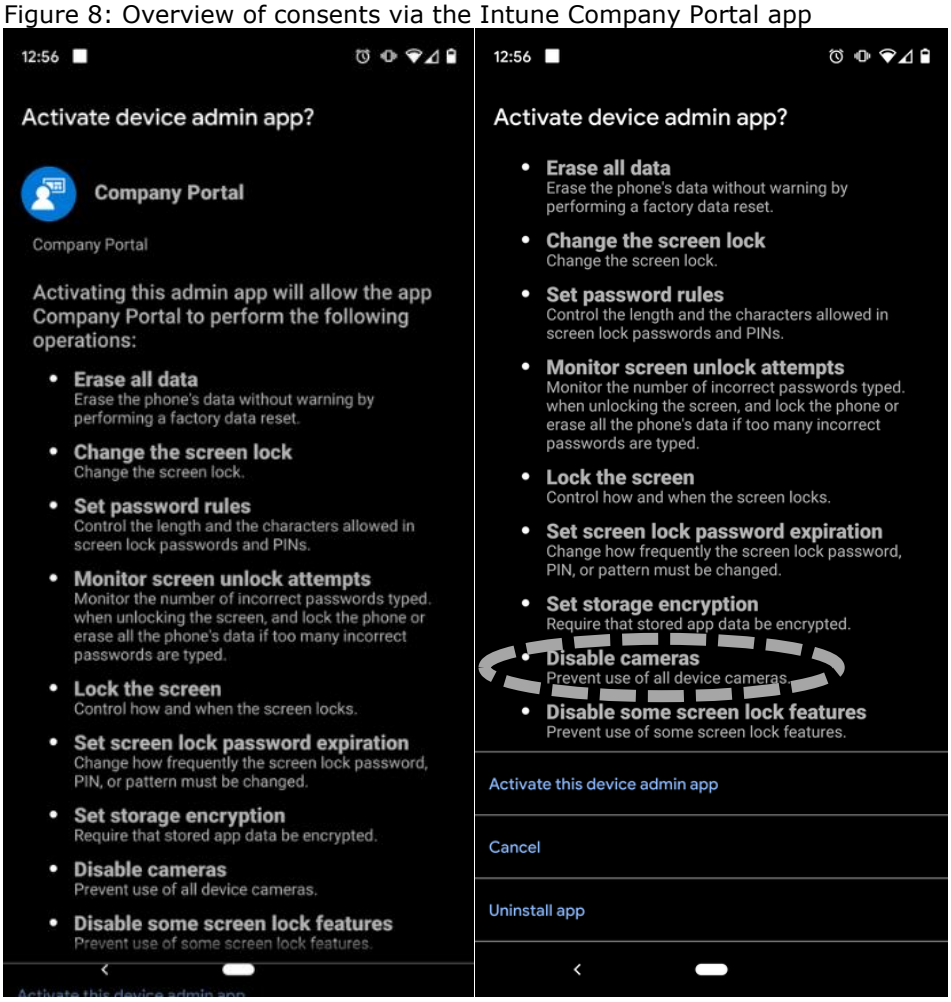


Then the app asks for consent to make phone calls (Figure 7).[34] The wording is unfortunate, as the app does not want to make phone calls but only needs access to the IMEI of the device.[35] Finally, the app states that it is able to turn off the camera (Figure 8). This could make it difficult for end-users to take screenshots of data, but this functionality was not turned on during the tests. It is not clear why the app asks for this consent.

[34] Microsoft describes all required steps, with screenshots at: https://docs.microsoft.com/en-gb/intune-user-help/enroll-device-android-company-portal. The steps for iOS are at this URL: https://docs.microsoft.com/en-gb/intune-user-help/install-and-sign-in-to-the-intune-company-portal-app-ios.

[35] Microsoft explains how administrators are able to help the users to understand asked permissions. Microsoft, Help end users understand Company Portal app messages, 9 March 2017, URL: https://docs.microsoft.com/en-gb/intune/fundamentals/end-user-company-portal-messages

Figure 8: Overview of consents via the Intune Company Portal app



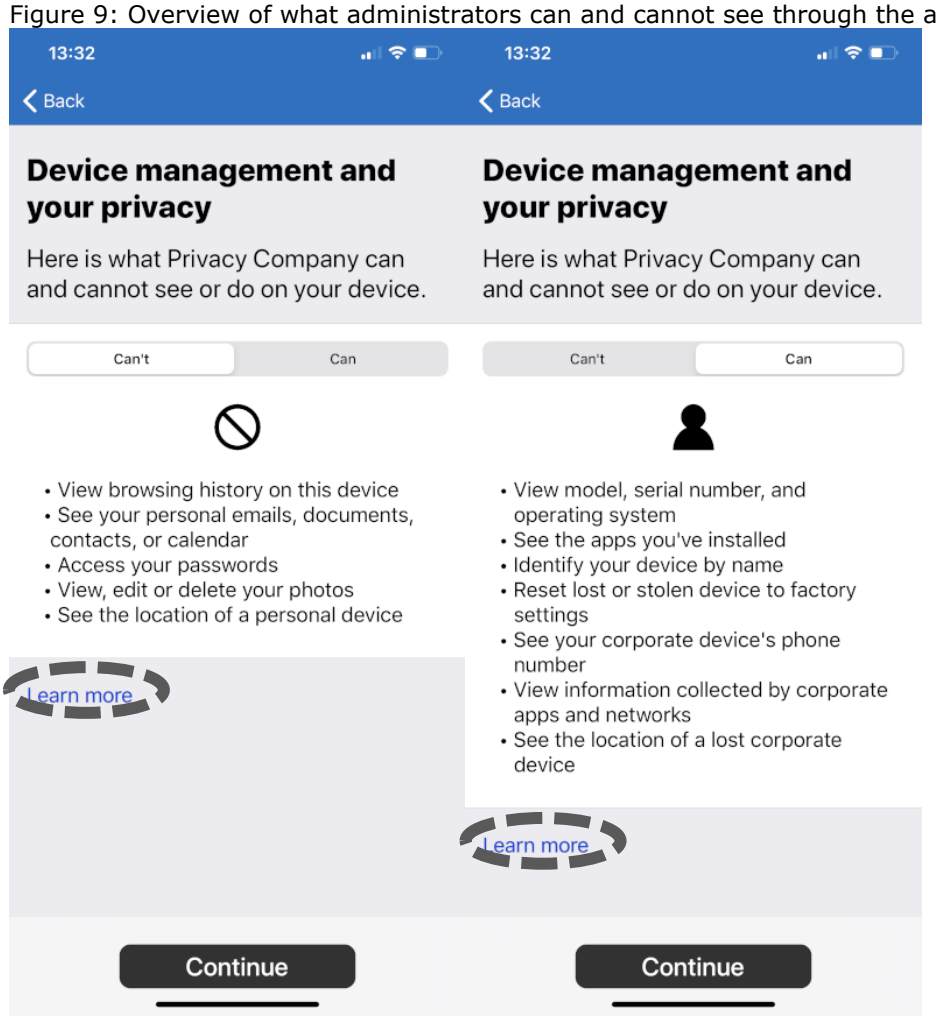
iOS and MacOS

As with Android devices, employees must also install the Company Portal app on their iOS and macOS devices.[36] On devices running iOS version 12.2 and higher, it is necessary to install a Management Profile.

Similar to the information on Android devices, employees also see an overview of the data and features that system administrators can and cannot access on Apple devices.

[36] Microsoft writes: "*Enrol your iOS device. Go to the App store to download and install the Intune Company Portal app on your device.*" URL: https://docs.microsoft.com/en-gb/intune-user-help/enroll-your-device-in-intune-ios#enroll-your-ios-device. Microsoft also writes: "*Install the Company Portal app on your iOS device to get access to your work and school apps, email, and network. Use the app to enrol your device in Microsoft Intune and secure its access to your work or school's resources.*" Microsoft, Install and sign in to the Company Portal app, 26 July 2019, URL: https://docs.microsoft.com/en-gb/intune-user-help/install-and-sign-in-to-the-intune-company-portal-app-ios. See: https://docs.microsoft.com/en-gb/intune-user-help/enroll-your-device-in-intune-macos-cp for the similar instruction for macOS.

Figure 9: Overview of what administrators can and cannot see through the app

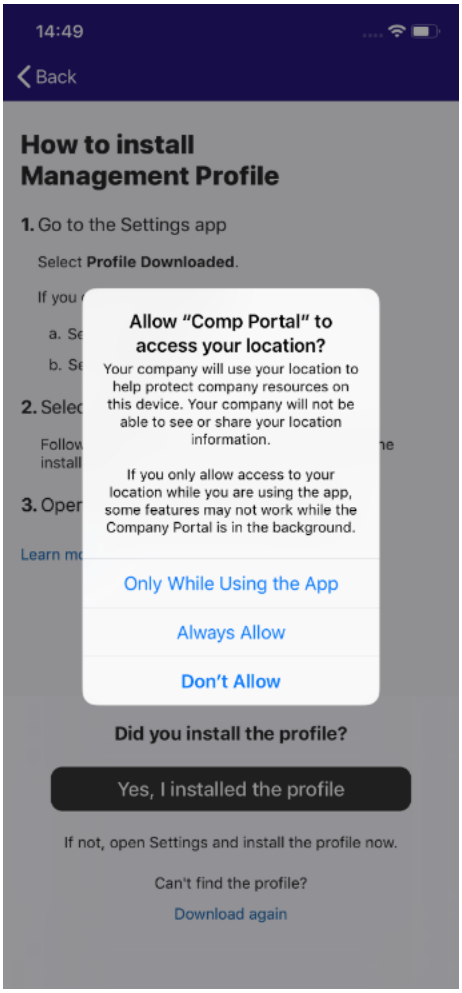


If users click on the Learn more link [circle added for clarity], they arrive at a Microsoft page with detailed information about the different permissions, what the organisation can never see, can always see and might be able to see.[37]

Initially, during the October 2019 tests, employees on iOS devices were asked if they wanted to give the Company Portal app access to their location data. Employees could refuse to do so without negative consequences, because they could continue with the installation if they chose 'Don't Allow'. In the March 2020 re-test, this question no longer appeared during installation, nor after the installation.

[37] Microsoft, What information can my organization see when I enroll my device? 31 October 2019, URL: https://docs.microsoft.com/en-gb/intune-user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune

Figure 10: Prior consent request for location information



It was verified that administrators cannot see location data if they change the status of a device from personal to corporate after the initial enrolment. They are not able to set the device to 'Lost', the first step in accessing location data. This is only possible for fully managed devices that have been enrolled out as such, via auto enrolment.

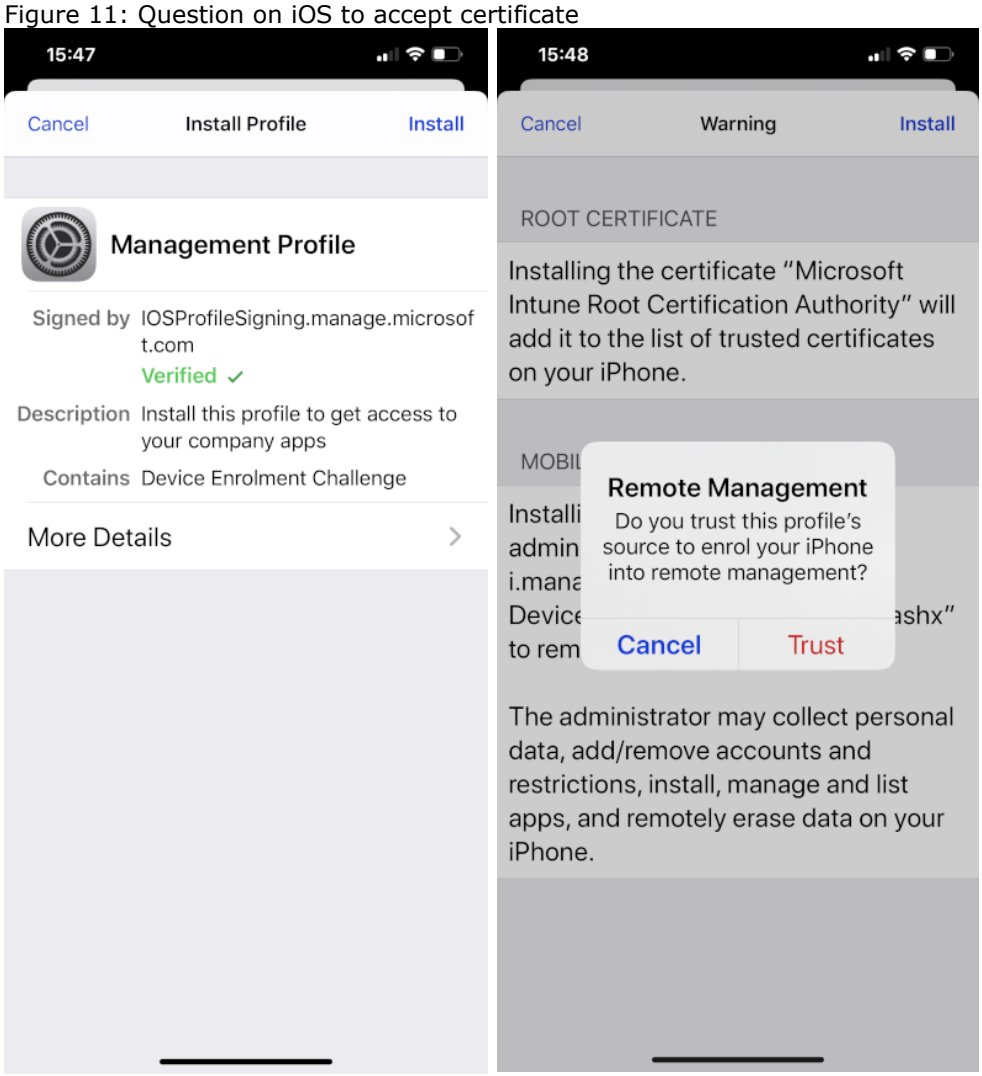
For each iOS user, system administrators must create a certificate for the first time. This certificate specifies certain management authorisations. After employees have logged into the Company Portal app, they must install the Management Profile. As part of this profile, they are asked to install and trust the certificate from the Microsoft Intune Root Certification Authority. System administrators can only perform the actions that are listed in this certificate.

Since iOS version 13, released mid-September 2019, Apple restricted the profile rules to the user (to a managed Apple ID) instead of to the device. This is also referred to as user enrolment instead of device enrolment. Apple restricted administrator access through Intune since this version.[38] For example, administrators can no longer view all installed apps. Administrators can no longer modify apps installed in a personal context to the corporate context. To do this, such a personal app must first be completely deleted. Also, the system administrators can no longer make any demands on the PIN code or reset or change the PIN code of the device remotely. As of iOS version 13, Apple no longer allows Intune to read unique identifiers of the device, such as the IMEI number. Finally, it is no longer possible to block the use of iCloud services as a backup.[39]

[38] "Under iOS 13, enrolled with User Enrollment, for example, a UEM will no longer be able to do the following:
Have an insight into the installed applications or the device identifier
Erase the device and the device password
Define complex password requirements (…)
With iOS 13, enterprise data, apps and policies are no longer bound to a single device, but to a managed Apple ID that can be created through Apple Business Manager and optionally connected to the Microsoft Azure Active Directory using Security Assertion Mark-up Language. Users can use their AD user credentials as a Managed Apple ID and log on to the device." Source: https://emea.mobi/ios-13-and-android-enterprise-simplify-the-use-of-byod-devices/

[39] Apple Support, iOS and iPadOS functionality restrictions, https://support.apple.com/guide/mdm/ios-and-ipados-restrictions-mdm0f7dd3d8/1/web/1. Also see: Microsoft, Intune support for new settings and updates in iOS 13 and macOS 10.15, URL: https://techcommunity.microsoft.com/t5/Intune-Customer-Success/Intune-support-for-new-settings-and-updates-in-iOS-13-and-macOS/ba-p/809055 Microsoft explains that the following 11 device restrictions will not be

Figure 11: Question on iOS to accept certificate



Windows

Unlike Android, iOS and macOS devices, employees don't need to install the Company Portal app on their self-managed Windows devices. They can also register their device via a browser in Intune.[40]

The technical inspection shows that Windows devices are automatically set to fully managed, instead of self-managed. Administrators will then be able to see all installed Microsoft apps. This is further explained in Section 3.1 (*Privacy choices Intune and Azure AD*).

possible anymore for personal devices, only for supervised devices: App Store, Explicit iTunes, music, podcast or news content, Adding Game Center friends, Multiplayer gaming, Camera, FaceTime, Safari, Autofill , Backup to iCloud, Block iCloud Document sync en Block iCloud Keychain sync. See the blog of a solution architect: "How to enrol an Apple device with iOS 13 "User Enrollment" mode in Microsoft Intune, 30 September 2019 URL: https://www.robinhobo.com/how-to-enroll-an-apple-device-with-ios-13-user-enrollment-mode-in-microsoft-intune/.

[40] See the Microsoft instructions how to enrol Windows devices, URL: https://docs.microsoft.com/en-gb/intune-user-help/using-your-windows-device-with-intune. Also: https://docs.microsoft.com/en-gb/intune/enrollment/windows-enrollment-methods

Azure AD
In the chosen test set-up all employees must use the Azure Active Directory (hereafter: Azure AD). This is Microsoft's online cloud identity service. Intune uses the Azure AD to recognise users instead of devices.

Even if government organisations use their own *on-premise* identity servers (local Active Directory servers), by linking to the Azure AD, Microsoft enables authentication with its own cloud services. Via the Azure AD, Microsoft processes at least the account data of individual employees and their login data. The use of Intune does in itself does not cause new types of data processing via the Azure AD. The difference is that Microsoft and the administrators can access historical log data much easier via the Azure AD log files than via other SIEM systems.

In SIEM systems and the Azure AD government organisations already collect data about the logging in and out of employees and the devices used for this, regardless of the use of Intune. However, the use of the Azure AD makes correlation with the other available data much easier. Therefore, this processing could pose additional risks to data subjects in combination with the Intune logs. For this reason the settings of the Azure AD and the audit logs about its use were included in this DPIA.

1.3 Difference between content, functional and diagnostic data

Inspired by the e-Privacy Directive, this report distinguishes between three categories of data processed by Microsoft as a service provider:

1. **Content** of communications with Microsoft services. Microsoft offers separate warranties for a part of this content data, under the heading 'Customer Data'. For Intune Customer Data are the inventory data from managed devices or information about the apps that are installed via Intune.[41]
2. **Diagnostic data**, all data that Microsoft stores in log files about the behaviour of individual users of its services. This includes the system-generated log files of Intune and the Azure AD, as well as the telemetry messages that are first collected via the Company Portal app on a laptop, tablet or smartphone and then sent to Microsoft.
3. **Functional data**, data that are only necessary for the transfer of communication. These data should be deleted or anonymised directly after completion of the transfer, according to the e-Privacy Directive.

Microsoft uses the term Customer Data for the content data that customers actively provide to Microsoft.

In this report, functional data refers to data that must be sent from the user's device in order to communicate with services on the Internet, including Microsoft's own apps and services. Examples of functional data are the data processed by an e-mail server and the necessary data flow to enable authentication of the user or the data that Microsoft needs to verify that the user has a valid license.

The main difference between functional data and diagnostic data is that functional data are and should be transient. As long as Microsoft does not store these

[41] Microsoft whitepaper, Intune Privacy and Data Protection Overview, March 2018, URL: http://download.microsoft.com/download/c/a/b/cab1f9bf-1c3f-41db-8994-5b0ea35dd846/intune_privacy_and_data_protection_overview.pdf. Microsoft writes: "*Customer Data is defined as "all data, including all text, sound, video or image files, and software that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. For example, this includes inventory information from managed devices or apps which have been installed through Intune."*

functional data, or if they are not personal data at the time of collection (for example because it concerns data about the temperature of a CPU in a server), they are not diagnostic data and fall outside the scope of this DPIA.

1.4 Privacy amendment SLM Rijk

Government organisations that belong to the Dutch central government (not the municipalities, nor the provinces) can use their existing Microsoft licenses under the conditions of the privacy amendment on the framework contract that SLM Rijk negotiated with Microsoft. For other Dutch government organisations that do not fall under this contract umbrella, there is a possibility to conclude a similar contract with similar privacy protections with Microsoft through a Dutch law firm that assisted SLM Rijk with the negotiations.[42]

Microsoft divides its Online Services into two categories: 'Core Services' and 'Other Online Services'. The Core Services are defined in the Online Service Terms (OST).[43] Since January 2020, Microsoft bundled its privacy guarantees for Enterprise services in a Data Protection Addendum.[44] In case of a conflict, the Dutch privacy amendment overrules the Online Service Terms and the Data Protection Addendum.

According to the OST, the Office Intune cloud software sometimes belongs to the Core Services, and sometimes to the Other Online Services (for example, when managed per device). When Intune is part of the Core Online Services, as part of Azure, Microsoft defines the service as follows: *"The cloud service portion of Microsoft Intune such as the Microsoft Intune Add-on Product or a management service provided by Microsoft Intune such as Mobile Device Management for Office 365."*[45] With this definition, Microsoft excludes data processing by locally installed software such as the Company Portal App.

The Dutch government privacy amendment applies to the processing of customer data and personal data through the use of all Microsoft Online Services procured under the Dutch government framework contract. Microsoft acknowledged that Office 365 ProPlus falls under this contract, as well as traffic that is actively sent from installed software such as Windows 10 and installed Office apps on mobile devices to Microsofts Online Service Services after a user has logged-in with a government work account. However, a recently commissioned DPIA relating to Office for the Web and the mobile Office apps shows that Microsoft does not apply the privacy amendment to the processing of all personal data associated with the mobile Office apps. SLM Rijk and Microsoft are engaged in a dialogue about the correct implementation by Microsoft of the contractual language in respect of all Online Services and to expand the improvements to other core Microsoft services used by the Dutch government.

The Dutch privacy amendment stipulates that Microsoft must act as a data processor for the processing of customer data and personal data received, collected, generated or derived through the use of the online services, except for

[42] Please contact Paul van den Berg with questions about this possibility, see the colophon for contact details.
[43] The most recent version of Microsofts' Online Service Terms for volume licensing dates from March 2020 and can be found here: https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=16205 .
[44] Microsoft Data Protection Addendum (DPA) for volume licensing of online services, January 2020, URL: https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=15981 Microsoft has not published a more recent version of the DPA since January 2020.
[45] Microsoft OST, March 2020 p. 26, Attachment 1 – Core online services.

the Controller Connected Experiences, when processing personal data for its own legitimate business interest and in respect of certain disclosures to authorities. This includes the use of Office 365 ProPlus as 'Other Online Service' and Intune. However, contrary to the privacy amendment, Microsoft does not apply the privacy improvements to services for which Microsoft still considers itself to be a data controller, such as Windows 10 Enterprise and the mobile Office apps.

The most important results of the privacy amendment are:

1. Microsoft acts as a data processor, and is limited to three purposes, where proportional, namely:
   1.to provide and improve the service,
   2.to keep the service up-to-date and
   3.secure.
   The amendment also specifies the business operations for which Microsoft is a data controller (such as invoicing).
2. Privacy guarantees apply to all kinds of personal data, not just contents of data actively uploaded by a customer, but also to telemetry and system generated log files.
3. Prohibition of the use of data for any kind of data analytics, profiling, marketing research or advertising. This includes the use of personal data to show personalised recommendations for products or services of Microsoft the government organisations have not purchased or do not use.
4. Amendment at the highest level of the enrolment framework.
5. SLM Rijk has effective audit rights and can exercise control over subprocessors.
6. If Microsoft anonymises personal data, it complies with the WP29 guidelines from WP216.

As explained above, the privacy amendment is applicable to all processing of customer data and personal data received, collected, generated or derived through the use of the online services. As the Company Portal app is a prerequisite to the use of the online service Intune, all processing of personal data associated with the Company Portal app when an employee uses the Azure AD, but also in other cases where a government organization wants to use Intune MAM with a local Azure AD, falls within the scope of the privacy amendment.[46]

These DPIA findings show that Microsoft does not apply the privacy amendment to the Company Portal app. Microsoft does not explicitly mention this anywhere, but this can be deduced from the following two circumstances:

1.
2. the reference to Microsoft's general privacy statement when installing the iOS/macOS and Android Company Portal app from the respective Apple and Google app stores and
3. the absence of the Company Portal apps in the various SOC and ISO audits on Intune, in combination with the limitation of the definition to the *cloud service portion*.

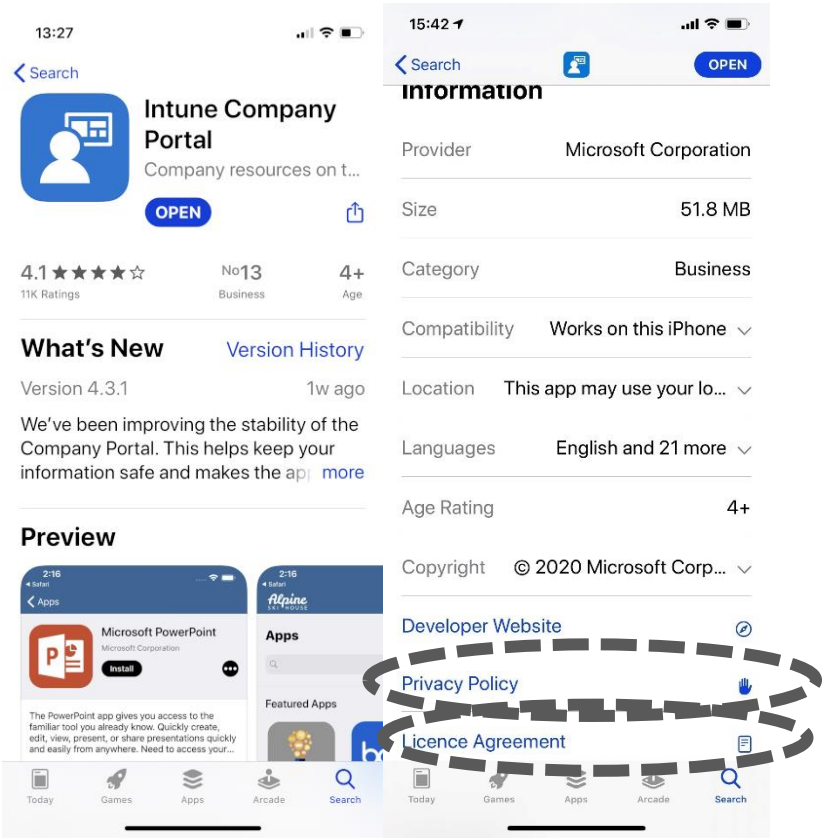
1.4.1 References in app stores to general Microsoft privacy statement

In the specific product terms in the Apple app store and in Google Play for the use of the Company Portal app, Microsoft refers to its general consumer privacy statement for the processing of data via the app.

[46] Though the use of MAM without enrolment (MAM-WE) was outside of the scope of this DPIA, the researchers note in section 1.2.3 that installation of the Company Portal App is required on Android devices in case of MAM-WE, but the employees do not have to log in.

Figure 12 shows what information Microsoft provides about the app in the app store, with links to its (general consumer) Privacy Policy and License Agreement [circle added for clarity].

Figure 12: Information privacy and licensing in the Company Portal app macOS and iOS



According to its (general) privacy statement, Microsoft is the controller of the data processing. In its privacy statement, Microsoft writes under the heading "*Products provided by your organization - Notification to end users*" that the organisation, such as the employer, is controller of the data processing and that in such cases the employee can only exercise his or her privacy rights with the employer.

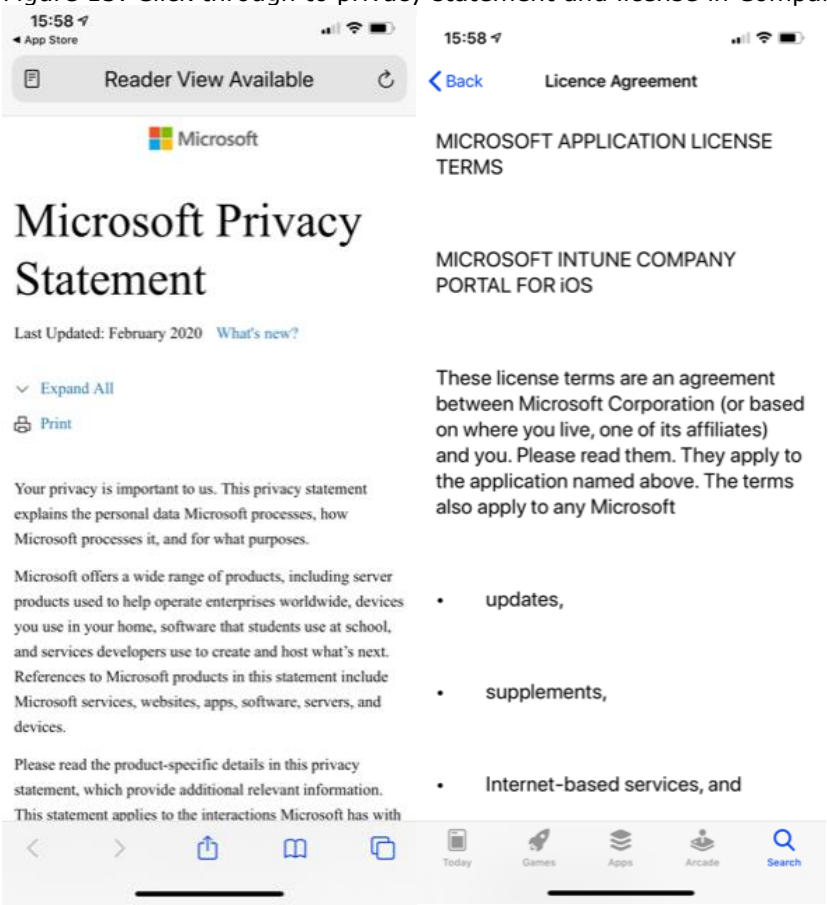
Microsoft writes, "*Many Microsoft products are intended for use by organisations, such as schools and businesses. Please see the Enterprise and developer products section of this privacy statement. If your organisation provides you with access to Microsoft products, your use of the Microsoft products is subject to your organization's policies, if any. You should direct your privacy inquiries, including any requests to exercise your data protection rights, to your organization's administrator. (…) When you use a Microsoft product provided by your organisation, Microsoft's processing of your personal data in connection with that product is governed by a contract between Microsoft and your organisation. Microsoft processes your personal data to provide the product to your organisation and you, and for Microsoft's legitimate business operations related to providing the product as described in the Enterprise and developer products section.*"[47] The hyperlinks to the Enterprise and Developer Products section describes cloud

[47] Microsoft privacy statement, last updated February 2020, URL: https://privacy.microsoft.com/en-GB/privacystatement

services, including Microsoft Intune, but does not mention the Company Portal app.[48]

In the information in the Appstore about the Company Portal app, Microsoft also writes that users can *not* contact Microsoft with questions about the app: "*If you have questions about how this app is being used within your organization), your company's IT administrator should have those answers for you. Microsoft, your network provider, and your device's manufacturer do not know how Intune will be used by your organization.*"[49]

Figure 13: Click through to privacy statement and license in Company Portal app



At the same time, Microsoft explains that users with a Windows platform should ask Microsoft for help, and not government organisations administrators if they need help with the Company Portal app: "*However, if you are not using Azure Government, the Company Portal for Windows 10 will send app logs directly to Microsoft when the user initiates the process to get help with an issue. Sending the app logs to Microsoft will make it easier to troubleshoot and resolve issues.*"[50]

In the separate license agreement for the Intune Company Portal app, as shown in Figure 13, Microsoft writes under the heading "*Usage Data*": "*Microsoft automatically collects usage and performance data over the internet. This data will*

[48] Idem, https://privacy.microsoft.com/en-GB/privacystatement#mainenterprisedeveloperproductsmodule
[49] Explanation in the Apple app store about the app.
[50] Microsoft, How to configure the Microsoft Intune Company Portal app, 24 February 2020, URL: https://docs.microsoft.com/en-gb/intune/apps/company-portal-app .

be used to provide and improve Microsoft products and services and enhance your experience. You can disable this feature."[51]

In response to earlier questions from SLM Rijk to Microsoft about the applicability of the OST to the mobile Office apps, Microsoft stated that all data that is provided to Microsoft via an Azure AD account are covered by the OST, which means that Microsoft only acts as a data processor. "*All Office Mobile applications are (indeed) offered under a EULA between Microsoft and the mobile device user, and the diagnostic data it collects is governed under the Microsoft Privacy Policy and the EULA. However, and crucially, data provided to Microsoft or collected by Microsoft through the use of an Azure AD Account authenticated in the Mobile apps are governed under the OST and your contract.*"[52]

In sum, given the fact that Microsoft applies its general privacy policy to the Company Portal App, **government organisations cannot assume that OST's and the privacy amendment's protection applies to the telemetry that Microsoft collects via the Company Portal app.**

1.4.2 No SOC and ISO audits on the Company Portal app

Microsoft has the data processing of its core Online Services audited under the strict audit regime of SOC 1 SSAE 18 and SOC 2 SSAE. The core services based on Azure, Intune included, have also been audited according to the SOC 3 standard.

The processing of data through Intune is part of the following four most recent audits:

- Microsoft Azure and Azure Government SOC 1 Type II Report (2018-07-01 to 2019-06-30)[53]
- Microsoft Azure & Azure Government SOC 2 Type II Report (2018-07-01 to 2019-06-30)[54]
- Microsoft Azure & Azure Government SOC 3 Report (2018-07-01 to 2019-06-39)[55]
- Microsoft Azure, Dynamics 365, and other Online Services - ISO 27001 and 27018 Assessment Report (20.12.2019).[56]

---

[51] Microsoft, How to configure the Microsoft Intune Company Portal app, 24 August 2016, URL: https://docs.microsoft.com/en-us/legal/intune/microsoft-intune-company-portal-application-license-terms

[52] Quoted in the DPIA Microsoft Office 365 Online and Mobile, SLM Rijk 23 July 2019, p. 31, URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/DPIA+Microsoft+Office+365+Online+and+Mobile+SLM+Rijk+23+july.pdf.

[53] Microsoft, New and Archived Audit Reports, can be reached through https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide . Microsoft describes this audit as follows: *"This document details audit assessment performed by a third party independent auditor on Azure and Azure Government systems, design, and operating effectiveness of controls that support SSAE18 and ISAE 3402 for the period 2018-7-1 through 2019-6-30. NOTE: Document is PDF Click Wrapped. Please download a local copy for better user experience."*

[54] Idem. Microsoft describes this audit as follows: "This document details audit assessment performed by a third party independent auditor on Azure systems, design, and operating effectiveness of controls that support SOC 2, AT 101, AICPA Trust Service objectives and principles, for the period 2018-7-1 through 2019-6-30. Also includes CSA STAR attestation and C5."

[55] Idem. "SOC 3 report for Microsoft Azure and Azure Government for the period 2018-7-01 through 2019-6-30."

[56] Idem. "Assessment report demonstrating Microsoft Azure, Dynamics 365, and other Online Services' compliance with the ISO 27001 and 27018 frameworks."

These audit reports do refer to the Intune cloud services, but do not to the Company Portal app.

The SOC 2 report contains the most comprehensive description of information security compliance for Identity and Access Management (IAM). This also includes access by Microsoft to the security and activity reports of the Azure AD, and the customer's own responsibility for, for example, issuing certificates and logging of unauthorised access.
It can be concluded that the Company Portal app and the built-in Intune functionality in Windows 10 Enterprise are granted a lower level of data protection than the Intune and Azure AD cloud services. Microsoft makes no audit reports available for the services for which Microsoft considers itself to be controller.

In sum, the lack of audits on the Intune Company Portal app also shows that Microsoft applies different legal conditions and privacy rules to the app than to the Intune cloud service.

2. Personal data and data subjects

2.1 Definitions of different types of personal data

Technically, Microsoft Corporation collects data about and through the use of Intune MDM and MAM in two different ways, namely (1) via the Company portal app and the similar built-in functionality in Windows 10 Enterprise and (2) via the Intune logs.

The app's outgoing traffic was intercepted and analysed as well as the various Intune logs after the two different test runs. The content of this traffic is described in detail in Sections 2.2, 2.3 and 2.4 of this report. In addition, Microsoft collects data on employee behaviour, such as log-in and log-out times via the Azure AD. Government organisations collect this information anyway, apart from the use of Intune. However, data processing via the Azure AD is discussed in this report, in Sections 1.2.3 (*Azure AD*), 2.4 (*Azure AD log files*), 3.1 (*Privacy choices Intune and Azure AD*) and 6 (*Interests in data processing*), because the administrators are capable of linking the data from the Intune log files to the Azure AD log files to get a more complete picture of the behaviour of employees. Such a combination of data could pose an additional risk to data subjects if no mitigating measures were taken.

Microsoft and government organisations process various types of personal data via Microsoft Intune, including the Company Portal app. The concept of personal data is defined in Article 4(1) of the GDPR as follows:

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

Microsoft collects personal data directly and indirectly.
Microsoft refers to the information it collects directly from customers as 'Customer Data'. Microsoft defines this term as follows: *"Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to*

Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Professional Services Data."[57] With this, Microsoft means the data that a customer knowingly provides for storage in a cloud service. In the privacy amendment negotiated SLM Rijk, and in the newly added Data Protection Addendum that is available for all worldwide volume licensing customers, Microsoft explicitly acknowledges that diagnostic data and system generated data can be personal data as well.[58]

Under the heading 'Processing of personal data; GDPR'[59] in the DPA, Microsoft states that the Customer's Data are personal data. Microsoft writes:

"*All Personal Data processed by Microsoft in connection with the Online Services is obtained as either Customer Data, Diagnostic Data, or Service Generated Data. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Online Service is also Customer Data. Pseudonymized identifiers may be included in Diagnostic Data or Service Generated Data and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data."*[60]

Microsoft confirms that pseudonymous or deidentified data may be generated by the use of the online services, and that these are personal data. Microsoft does not provide definitions of pseudonymisation, anonymisation or de-identification, nor does Microsoft explain what types of data it may 'derive' from personal data.

In a specific explanation about Intune, Microsoft describes that the company processes three types of data via Intune, namely (1) identified data about the user and the device, (2) pseudonymised data such as diagnostic data and system generated data, plus data that are linked to a unique identifier and (3) aggregated data.[61]

Microsoft collects these data from the following sources:

- *"The admin's use of the Intune in the Azure portal.*
- *End-user devices (when they enroll for Intune management and during usage).*
- *Customer accounts at third party services (per the admin's instructions).*
- *Diagnostic, performance, and usage information."*[62]

Microsoft does not explain what diagnostic data it collects through the telemetry flow from the Company Portal app, and uses the term 'pseudonymized data' without acknowledgment of the fact that under the GDPR, the processing of pseudonymised data, is processing of personal data. In the improved privacy terms negotiated by SLM Rijk, the privacy guarantees are explicitly extended to

[57] Microsoft OST, March 2020, Definitions, p. 4.
[58] Microsoft, Data Protection Addendum, January 2020, URL: https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=15981
"Diagnostic Data" means data collected or obtained by Microsoft from software that is locally installed by Customer in connection with the Online Service. Diagnostic Data may also be referred to as telemetry. Diagnostic Data does not include Customer Data, Service Generated Data, or Professional Services Data. "Service Generated Data" means data generated or derived by Microsoft through the operation of an Online Service. Service Generated Data does not include Customer Data, Diagnostic Data, or Professional Services Data.
[59] Ibidem.
[60] Ibidem.
[61] Microsoft, Data collection in Intune, 18 May 2018, URL: https://docs.microsoft.com/en-GB/intune/protect/privacy-data-collect
[62] Idem.

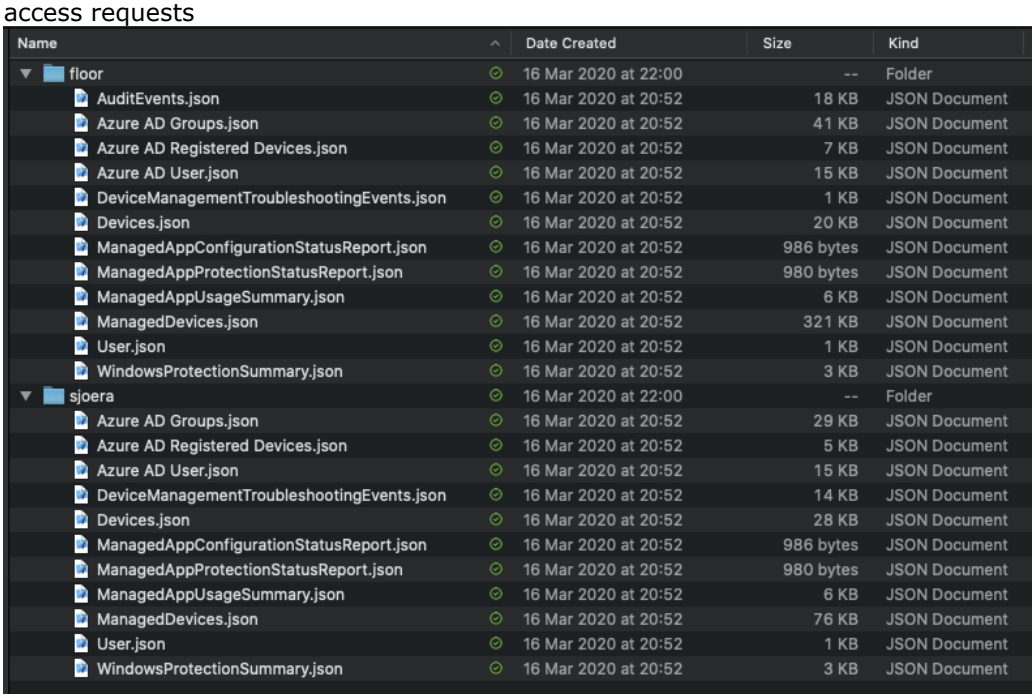
all types of diagnostic data about the individual use of the Microsoft services, including telemetry data from installed software and apps.

2.2 Three types of Intune log files

Since February 2019, Microsoft has been publishing extensive documentation on the content of diagnostic messages that it collects via the cloud services Intune MDM and MAM, for example on the compliance policy on iOS[63], Android[64], Windows 10[65] and macOS.[66]

Intune collects this diagnostic data in three different types of log files, namely: Audit logs, Operational logs, and Organisational logs for device compatibility. Government organisations used the Export-IntuneData.ps1 script to run the files in the test user's name.[67] All three types of log files were reviewed and compared with the executed test scenarios.

Figure 14: Various Intune log files retrieved in the name of the test users via digital access requests



Name	Date Created	Size	Kind
floor	16 Mar 2020 at 22:00	--	Folder
AuditEvents.json	16 Mar 2020 at 20:52	18 KB	JSON Document
Azure AD Groups.json	16 Mar 2020 at 20:52	41 KB	JSON Document
Azure AD Registered Devices.json	16 Mar 2020 at 20:52	7 KB	JSON Document
Azure AD User.json	16 Mar 2020 at 20:52	15 KB	JSON Document
DeviceManagementTroubleshootingEvents.json	16 Mar 2020 at 20:52	1 KB	JSON Document
Devices.json	16 Mar 2020 at 20:52	20 KB	JSON Document
ManagedAppConfigurationStatusReport.json	16 Mar 2020 at 20:52	986 bytes	JSON Document
ManagedAppProtectionStatusReport.json	16 Mar 2020 at 20:52	980 bytes	JSON Document
ManagedAppUsageSummary.json	16 Mar 2020 at 20:52	6 KB	JSON Document
ManagedDevices.json	16 Mar 2020 at 20:52	321 KB	JSON Document
User.json	16 Mar 2020 at 20:52	1 KB	JSON Document
WindowsProtectionSummary.json	16 Mar 2020 at 20:52	3 KB	JSON Document
sjoera	16 Mar 2020 at 22:00	--	Folder
Azure AD Groups.json	16 Mar 2020 at 20:52	29 KB	JSON Document
Azure AD Registered Devices.json	16 Mar 2020 at 20:52	5 KB	JSON Document
Azure AD User.json	16 Mar 2020 at 20:52	15 KB	JSON Document
DeviceManagementTroubleshootingEvents.json	16 Mar 2020 at 20:52	14 KB	JSON Document
Devices.json	16 Mar 2020 at 20:52	28 KB	JSON Document
ManagedAppConfigurationStatusReport.json	16 Mar 2020 at 20:52	986 bytes	JSON Document
ManagedAppProtectionStatusReport.json	16 Mar 2020 at 20:52	980 bytes	JSON Document
ManagedAppUsageSummary.json	16 Mar 2020 at 20:52	6 KB	JSON Document
ManagedDevices.json	16 Mar 2020 at 20:52	76 KB	JSON Document
User.json	16 Mar 2020 at 20:52	1 KB	JSON Document
WindowsProtectionSummary.json	16 Mar 2020 at 20:52	3 KB	JSON Document

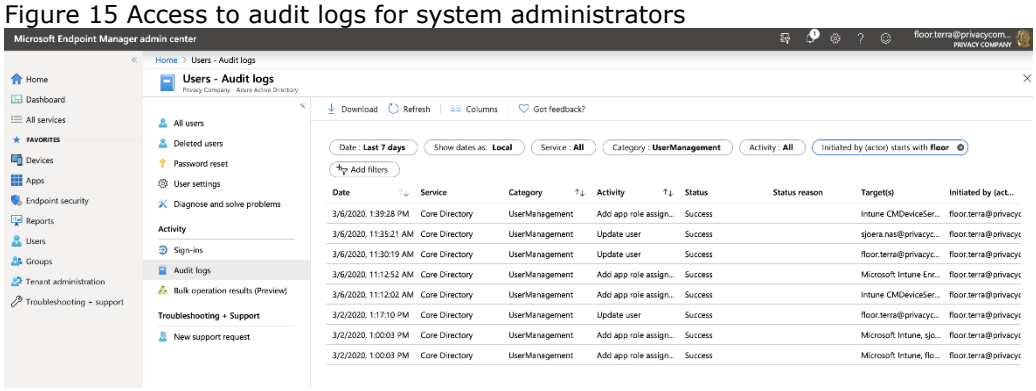
Because the research was done on a tenant with a combination of MDM and MAM, it is not possible to make a technical distinction in this DPIA between log files that

[63] Microsoft, iosCompliancePolicy resource type, 4 March 2020, URL: https://docs.microsoft.com/en-gb/graph/api/resources/intune-deviceconfig-ioscompliancepolicy?view=graph-rest-1.0
[64] Microsoft, androidCompliancePolicy resource type, 4 March 2020, URL: https://docs.microsoft.com/en-gb/graph/api/resources/intune-deviceconfig-androidcompliancepolicy?view=graph-rest-1.0
[65] Microsoft, windows10CompliancePolicy resource type, 4 March 2020, URL: https://docs.microsoft.com/en-gb/graph/api/resources/intune-deviceconfig-windows10compliancepolicy?view=graph-rest-1.0
[66] Microsoft, macOSCompliancePolicy resource type, 4 March 2020, URL: https://docs.microsoft.com/en-gb/graph/api/resources/intune-deviceconfig-macoscompliancepolicy?view=graph-rest-1.0
[67] Administrators can invoke this powershellscript via URL: https://aka.ms/intunedataexport. Microsoft mentions this script on an information page about Data Subject Access Requests, URL: https://docs.microsoft.com/en-gb/intune/protect/privacy-data-audit-export-delete

relate to MDM and log files that relate to MAM. A provisional distinction can be made on the name of the log files. Files containing the word device have been assigned to Intune MDM, files containing the word app have been assigned to Intune MAM. See Figure 14.

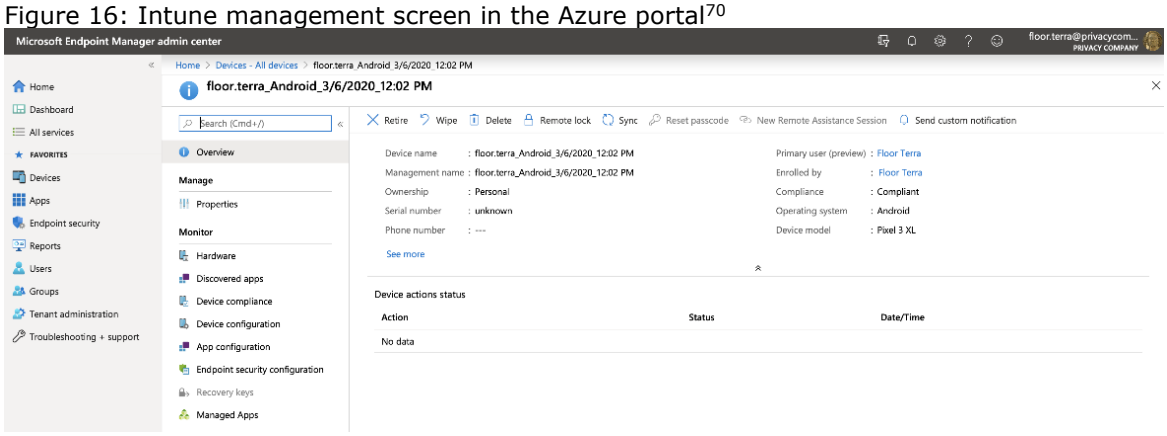
The **Auditlogs** show details about each event or task in the own Intune environment. Microsoft writes: "*Audit logs contain a list of activities that generate a change in Microsoft Intune. The actions create, update (edit), delete, assign, and external actions provide control events that administrators can view for most of Intune's workloads. By default, control is enabled for all customers. The feature cannot be disabled. (..)* ***By default, the last 30 days of audit events are displayed****. (..) See List auditEvents for more information about using the Graph API* ***to retrieve one year of audit events****.*"[68]

Figure 15 Access to audit logs for system administrators



In a slightly older publication, Microsoft writes, *"For security purposes Intune may maintain audit logs for user and device actions for a period of one year. These logs are automatically deleted after the one-year retention period."*[69]

Figure 16: Intune management screen in the Azure portal[70]



The **operational logs** contain information about the (successful or unsuccessful) registration of users and devices. In the **organisational logbooks for device**

[68] Microsoft, Use audit logs to track and monitor events in Microsoft Intune, 18 March 2019, URL: https://docs.microsoft.com/en-gb/intune/fundamentals/monitor-audit-logs
[69] Microsoft, Audit, export, or delete personal data in Intune, 18 May 2018, URL: https://docs.microsoft.com/en-gb/intune/protect/privacy-data-audit-export-delete
[70] This management screen can be reached through https://portal.azure.com.

compatibility an organisational report is displayed for device compatibility is in Intune and information about incompatible devices.[71]

The data in the log files were compared with the executed test scenarios. Only the last status of the device is shown in the log files. It is not possible to see a historical overview of status changes. Government organisations may choose to set export options. This would allow the government organisations to keep the log files longer than the default value of 30 days.

2.2.1 Microsoft Intune MDM

Through Intune MDM, Microsoft and the system administrators collect information about general characteristics of the registered devices. This includes information such as the model, serial number, operating system, names of installed apps managed through Intune, and the user chosen device name.

Microsoft explains what information an administrator can and cannot see through Intune.[72]
What administrators can never see:

- Calling and web browsing history
- E-mail and text messages
- Contacts
- Calendar
- Passwords
- Pictures, including what's in the photos app or camera roll
- Files[73]

Microsoft explains that system administrators of government organisations can see the following types of data of self-managed devices:

- Device model, like Google Pixel
- Device manufacturer, like Microsoft
- Operating system and version, like iOS 12.0.1
- App inventory and app names managed by Intune, like Microsoft Word. On personal devices, your organization can only see your managed app inventory. On corporate-owned devices, your organization can see all of your app inventory.
- Device owner
- Device name
- Device serial number
- UDID, MEID and Intune Device ID (unique device identifiers)
- Total available and free storage space on the device
- Enrolled date and date of last contact with Intune[74]

[71] Microsoft, Send log data to storage, event hubs, or log analytics in Intune (preview), 18 February 2020, URL: https://docs.microsoft.com/en-gb/intune/fundamentals/review-logs-using-azure-monitor
[72] Microsoft, What information can my organisation see when I enroll my device? 31 October 2019, URL: https://docs.microsoft.com/en-gb/intune-user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune
[73] Idem.
[74] These latter three categories of information are not mentioned on the main information page, but can be found in a separate (not linked) overview of all hardware device details Microsoft can read through Intune. Microsoft, Device details in Intune, 27 February 2020, URL: https://docs.microsoft.com/en-gb/intune/remote-actions/device-inventory.

The technical inspection of the Intune log files shows that Microsoft and the system administrators also collect the following data:

- userID
- e-mail address
- e-mail alias

Microsoft explains what administrators can sometimes see through Intune:

- Phone number: For corporate-owned devices, your full phone number is visible. For personal-owned devices, just the last four digits of your phone number are visible to your organisation. You can see the ownership type of each device on its Device Details page.
- Device storage space: If you can't install a required app, your organisation might look at your device's storage space to figure out if space is too low.
- Location: Your organisation can never see your device's location, unless you need to recover a lost, supervised iOS device.
- App inventory details: If your organisation uses Mobile Threat Defense, more details will be shown about the apps that are installed on your iOS-device.
- Network information: Certain information about network connections for Android devices may be available to your organisation for support. For example, if your organisation requires devices to remain within a certain building, your device identifies the network to which it is connected.[75]

Government organisations have to assess the necessity to collect device storage space, and decide whether they need to manage the devices in a personal, or in a corporate mode. This is part of the specific data protection risk assessment they need to perform based on this umbrella DPIA.

As explained in Section 1.2.2 (Microsoft Intune Company Portal App), administrators can change the status of devices registered in Intune MDM from personal to corporate. A test was conducted for this DPIA to see what additional data Microsoft collects in the log files after such a status change. The results of this test are discussed in Section 3.1.1 of this report (*Privacy choices Intune and Azure AD*).

Table 2: unique identifiers found in the MDM log files [March 2020]

Identifiers/ platform	**Windows 10**	**macOS 10.15.3**	**Apple iOS 13.3.1**	**Android 10**
userId	fdb22d51-b362-4946-a116-8b440de11a30	234783b6-e703-4ba2-9772-69042325bab7	fdb22d51-b362-4946-a116-8b440de11a30	234783b6-e703-4ba2-9772-69042325bab7
Device Name	FIT-LT00095	Floor's MacBook Pro	iPhone XS	floor.terra_Android_3/6/2020_12:02 PM
lastSyncDateTime	2020-03-06T17:22:04.7073012Z	2020-03-06T21:04:59.416075Z	2020-03-06T15:37:36.4044769Z	2020-03-06T15:18:12.0232166Z

[75] Microsoft, What information can my organization see when I enroll my device?, 31 October 2019, URL: https://docs.microsoft.com/en-gb/intune-user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune.

E-mail Address	sjoera.nas@[anonymised].nl	floor.terra@[anonymised].nl	sjoera.nas@[anonymised].nl	floor.terra@[anonymised].nl
userPrincipalName	sjoera.nas@[anonymised].nl	floor.terra@[anonymised].nl	sjoera.nas@[anonymised].nl	floor.terra@[anonymised].nl
imei	null	null	[geanonimiseeerd]	null
serial Number	J8R7NN2	C02X983QJG5J	FFMXVAP6KPH2	unknown
UserDisplayName	Sjoera Nas	Floor Terra	Sjoera Nas	Floor Terra
wiFiMac Address	[anonymised]	[anonymised]	[anonymised]	[anonymised]
meid	null	null	35729909994076	null
MAC-adres	"ethernetMacAddress": "[anonymised]",	"ethernetMacAddress": "[anonymised]",		
Detected apps			Comp Portal	Company Portal

The Intune MDM log messages are personal data, because each message contains a number of direct and indirect identifying data, namely: the e-mail address and the e-mail alias, the name of the owner of the device, the self-chosen device name, the serial number of the device and the IMEI. In addition, Microsoft automatically collects the IP addresses of the self-managed devices.

Microsoft is able to identify an individual user on the basis of this information in the various messages that Microsoft collects, and retains it as long as the registration is not actively removed by government organisations administrators.

2.2.2 Microsoft Intune MAM

Through the Intune log files, Microsoft and government organisations collect the following types of data:

- IMEI
- Account name (e-mail address and e-mail alias)
- Other identifiers, such as serial number, device name and azureActiveDirectoryDeviceId
- Last login user

Table 3: unique identifiers found in the Intune log files [March 2020]

Identifiers/ Platform	**Windows 10**	**macOS 10.15.3**	**Apple iOS 13.3.1**	**Android 10**
IMEI	null	null	357299099940766	null

Account Name	sjoera.nas@[anonymised].nl	floor.terra@[anonymised].nl	sjoera.nas@[anonymised].nl	floor.terra@[anonymised].nl
Other Identifiers	"NetBiosName": "FIT-LT00095","Manufacturer": "Dell Inc.","Model": "Latitude 5480","SerialNumber": "J8R7NN2",	"NetBiosName": "Floorâ□□s MacBook Pro", "Manufacturer": "Apple","Model": "MacBook Pro","SerialNumber": "C02X983QJG5J",	"NetBiosName": "iPhone XS","Manufacturer": "Apple","Model": "iPhone XS Max","SerialNumber": "FFMXVAP6KPH2",	"NetBiosName": "floor.terra_Android_3/6/2020_12:02 PM","Manufacturer": "Google","Model": "Pixel 3 XL","SerialNumber": "unknown",
Last login User	"usersLoggedOn": [{"userId": "fdb22d51-b362-4946-a116-8b440de11a30","lastLogOnDateTime": "2020-03-16T19:31:18.873Z"}],	"usersLoggedOn":[{"userId": "234783b6-e703-4ba2-9772-69042325bab7", "lastLogOnDateTime": "2020-03-16T12:19:04.155Z"}],	"usersLoggedOn": [{"userId": "fdb22d51-b362-4946-a116-8b440de11a30","lastLogOnDateTime": "2020-03-16T14:13:38.013Z"}],	"usersLoggedOn":[{"userId": "234783b6-e703-4ba2-9772-69042325bab7","lastLogOnDateTime": "2020-03-16T20:20:31.766Z"}],

Intune MAM log messages are personal data, because each message contains a number of direct and indirect identifying data, namely: the e-mail address and e-mail alias, the chosen device name, the serial number of the device and the IMEI. In addition, Microsoft automatically collects the IP addresses of the self-managed devices.

Microsoft is able to identify an individual user on the basis of the information in the various messages that Microsoft collects, and retains it as long as the registration is not actively removed by government organisations administrators.

2.3 Data processed by Microsoft through the Company Portal app

Through the Intune Company Portal app, Microsoft records information about the device and the user of the app. Microsoft regularly sends that information, in batches, to Microsoft's servers in the United States. These are telemetry data. Actually, there are two types of telemetry data: the data about the functioning of the device needed to provide the Intune service, which are also visible in the log files described in the previous section, and the telemetry data that Microsoft apparently collects for its own purposes. The telemetry data are automatically sent to Microsoft without user intervention.

In addition, Microsoft collects a separate log file on the device, a debug log, in order to detect errors in the operation of the app. In the event of a malfunction, the user can send this file to Microsoft. Debug logs are a comprehensive record of events that occur when running the Company Portal app. With a user's consent, the debug log can be sent to Microsoft or government organisations

administrators.[76] The difference with the telemetry data is that the debug log contains other data and more technical details about the internal operation of the Company Portal app.

Microsoft does not provide separate information about the nature of these two types of data processing, and the types of personal data it processes in this way. Microsoft provides one very brief explanation in the general Intune manual by type of device, under the heading 'Turn off Microsoft usage data collection'. Microsoft writes, " *Microsoft automatically collects certain data about products and services. The data is used to improve the reliability and performance of apps, like Company Portal and Microsoft Intune. Even though this data is anonymized, some users may not feel comfortable with this collection*."[77] Microsoft explains how users in the app can turn off data sharing themselves. Microsoft only refers to the telemetry data with this, because it does not mention the debug logs. Microsoft explains that the administrators have no control over the transmission of the telemetry data. They cannot turn off this data collection centrally, for example by means of a group policy.[78] Microsoft does not explain whether there are control options for the debug logs.

Privacy Company analysed the data that have been recorded with the Company Portal app on two of the platforms: iOS and macOS. 9 and 10 telemetry messages sent from the iOS and macOS Company Portal app were sent respectively.

The telemetry data sent from Android could not be decoded. The Android app applies *certificate pinning* in a way that cannot be technically circumvented without removing (rooting) the security in the device's operating system. In the second test run, in March 2020, Microsoft had also added certificate pinning to the app on macOS.[79]

Because Windows 10 Enterprise has in-built Intune functionality, devices can be registered with a browser. Users do not need to install the separate Company Portal app. It is technically not possible to distinguish between the telemetry flow from Windows 10 and the telemetry flow from the in-built Intune functionality. However, users can influence the telemetry flow via the general telemetry setting in Windows 10. This is explained in Section 3.1 (*Privacy choices Intune and Azure AD*).

From iOS and macOS, the app transmits the telemetry data to the Microsoft domain mobile.pipe.aria.microsoft.com.[80]

[76] Microsoft, Turn off Microsoft usage data collection [on Android], 19 April 2019, URL: https://docs.microsoft.com/en-gb/intune-user-help/turn-off-microsoft-usage-data-collection-android
[77] Idem.
[78] Idem. "Your organization doesn't have control over the collection of this data, and they can't change your setting selection."
[79] It might be possible to bypass the certificate pinning with a debugger, like Frida, but the results are not certain and in any case very labour-intensive.
[80] IP-address 52.114.132.74, owned by Microsoft in Washington, Virginia. See: https://www.ip-tracker.org/locator/ip-lookup.php?ip=Mobile.pipe.aria.microsoft.com. No traffic was sent to the other known Microsoft domain on which it processes, for example, telemetry data from Windows 10, watson.telemetry.microsoft.com.

Telemetry data collected via iOS and macOS during the first test run in September and October 2019

1. iOS
    a. Telemetry sent to mobile.pipe.aria.microsoft.com and gate.hockeyapp.net
    b. Functional traffic to fef.amsub0102.manage.microsoft.com, login.microsoftonline.com, enterpriseregistration.windows.net and graph.windows.net
    c. Microsoft detected and logged that a Mitm proxy was used to intercept traffic to Microsoft and logged the entire public section of the certificate.
    d. During the test sessions, the following telemetry events were observed:
        i. ios_session
        ii. adalworkflow
        iii. useraction
        iv. outgoingservicerequest
        v. pageaction
        vi. appstatechange
        vii. session
        viii. completedloginworkflow
        ix. applifecycle
        x. inappprocess
2. macOS
    a. Telemetry sent to mobile.pipe.aria.microsoft.com and gate.hockeyapp.net
    b. Functional traffic to login.microsoftonline.com and enterpriseregistration.windows.net
    c. Microsoft detected and logged that a Mitm proxy was used to intercept traffic to Microsoft.
    d. During the test sessions, the following telemetry events were observed:
        i. session
        ii. completedloginworkflow
        iii. pageaction
        iv. macos_session
        v. useraction
        vi. applifecycle
        vii. adalworkflow
        viii. outgoingservicerequest
        ix. inappprocess

Telemetry data collected via iOS during the second test run in March 2020. On macOS observation was not possible anymore, due to certificate pinning.

1. iOS
    a. Telemetry sent to mobile.pipe.aria.microsoft.com and gate.hockeyapp.net
    b. Functional traffic to fef.amsub0502.manage.microsoft.com, login.microsoftonline.com, enterpriseregistration.windows.net and graph.windows.net and i.manage.microsoft.com
    c. Microsoft detected and logged that a Mitm proxy was used to intercept traffic to Microsoft and logged the entire public section of the certificate.
    d. During the test sessions, the following telemetry events were observed:

i. session
ii. applifecycle
iii. bios_session
iv. appstatechange
v. inappprocess
vi. pageaction
vii. useraction
viii. outgoingservicerequest

From the Company Portal app, traffic is also sent to the U.S. hosted domain gate.hockeyapp.net, recently procured by Microsoft, and since referring to Microsoft's own domain: https://appcenter.ms/. According to this website, this service monitors the functioning of apps on each platform (Crash analytics).

The following POST request to Hockeyapp on iOS was observed in March 2020:
{"iKey":"4c723906-7519-48fe-8469-32fef395363b","name":
"Microsoft.ApplicationInsights.SessionState","time":"2020-03-
06T12:32:17.381Z", "data":{"baseData":{"ver":2,"state":0},
"baseType":"SessionStateData"}
,"ver":1,"sampleRate":100,"tags":{"ai.device.screenResolution":"2688x1242","ai
.user.id":"2846210D-874A-4DE1-A545-
A6F80F5CBFA0","ai.device.locale":"en_NL",
"ai.device.model":"iPhone11,6","ai.application.ver":"4.3.1 (51.2002021.000)",
"ai.device.type":"Phone",
"ai.internal.sdkVersion":"ios:5.1.4","ai.device.oemName"
:"Apple","ai.device.osVersion":"13.3.1 (17D50)","ai.session.isFirst":"false",
"ai.device.id":"2846210D-874A-4DE1-A545-A6F80F5CBFA0","ai.session.id"
:"54A0CAD3-91DE-409B-A735-C67F5CC94453","ai.device.language"
:"en","ai.session.isNew":"true","ai.device.os":"iOS"}}

In connection with the IP addresses that Microsoft automatically collects when sending, these telemetry messages from the Intune Company Portal Office app are personal data because each message contains one or more unique device identifiers and a timestamp. This information is linked to information about the use of a managed Microsoft application, depending on the type of action the user performs.

Microsoft is able to identify an individual user **on the basis of the information contained in the various messages, such as the DeviceInfo.Id device identifier included in each telemetry message**, which Microsoft collects and stores for at least 90 days (see Section 10 of this report, *Retention periods*). Microsoft, as a specialised technology company, must be reasonably able to link individual user messages through the account information, unique device identifier, and timestamp, and thus to directly or indirectly identify data subjects.

In 2017, the Dutch Data Protection Authority (DPA) assessed that the telemetry data that Microsoft collects through Windows are personal data. During this investigation, Microsoft stated that most of the telemetry data did not relate to individuals, but to (technical aspects of) the operating system.[81] As explained in section 2.1 of this report (*Definitions of different types of personal data*), Microsoft

[81] Dutch DPA, report of findings Windows 10 Home and Pro, in Dutch: rapport definitieve bevindingen Microsoft Windows 10, de verwerking van persoonsgegevens via telemetrie, p. 101, URL: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/01_onderzoek_microsoft_windows_10_okt_2017.pdf

now recognises in its Online Service Terms, specifically the new Data Protection Addendum, that diagnostic data may contain personal data.

An example of a (part of a) log line in the debug log on an app on Android[82], without visible content, is:

},"Key@odata.type":"Edm.Guid**","Key":"69a4ce05-ab42-4a7a-baf7-7a8f76dde081"**,"ChassisType":"Phone","Nickname":null,"DeviceHWId":null,"Manufacturer":"Google","Model":"Pixel 3 XL",**"OfficialName":"floor.terra_Android**_3/6/2020_12:02 PM","OperatingSystem":"Android","ManagementType":"Mdm","RemotableProperties":null,"ManagementAgent":"Mdm","LastContact@odata.type":"Edm.DateTime**","LastContact":"2020-03-06T15:18:12.0232166"**,"LastContactNotification@odata.type":"Edm.DateTime", "LastContactNotification":"0001-01-01T00:00:00","ComplianceState":"Compliant", "NoncompliantRules":[

Each log line starts with a date timestamp, and also contains a unique userID. In connection with the IP addresses that Microsoft automatically collects when sending the debugs, these log files from the Intune Company Portal Office app are also personal data, because the messages contain a unique identifier (the 'key'), the UserID, a readable name of a user and a date-time stamp.

2.4 Azure AD log files

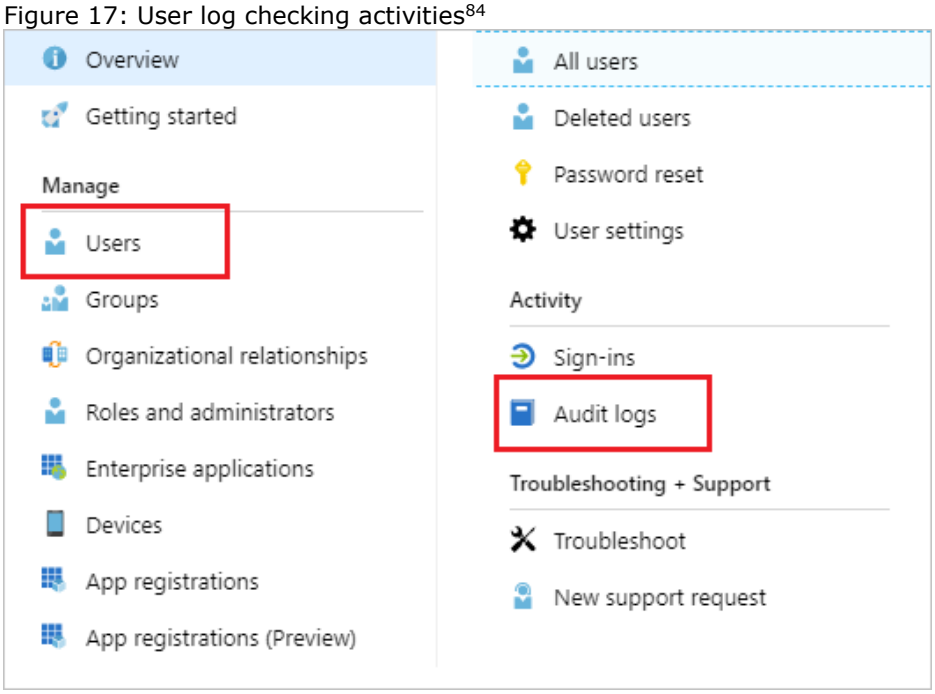
Microsoft collects and processes two types of personal data on the use of the Azure Active Directory

The first category of personal data are log files that Microsoft collects and processes for its own purposes. These purposes are explained in Section 4.4 of this report (*Current Purposes Azure AD*). Microsoft acknowledges that the log files contain personal data, but writes that it will remove these personal data from the log files (*scrubbing*) before processing the data in the machine learning systems for general analysis.

Microsoft writes, "*Log files contain data about usernames, groups, devices, and apps. Log files are originally created and stored in Azure storage in the data center where the Azure AD service runs.*
Log files are used for local debugging, usage analysis, and system health monitoring purposes, as well as for service-wide analysis. Prior to any system-wide analysis, log files are first scrubbed of personal data, which is tokenized. These logs are then copied over a secure SSL connection to Microsoft's reporting machine learning systems, which are contained in Microsoft owned data centers in the Continental United States."[83]

[82] Recorded on 6 March 2020.
[83] Microsoft whitepaper, Ramiro Calderon, Azure Active Directory Data Security Considerations, Version: 1.01, Published: June 2018, URL: https://aka.ms/aaddatawhitepaper.

Figure 17: User log checking activities[84]



In addition, Microsoft describes that it records user login and system activity reports through the Azure AD. [85] Microsoft publishes detailed information about the content of the audit logs[86] and sign-in logs.[87] These reports are primarily intended for the system administrators, but Microsoft also processes these reports for its own purposes.

Microsoft describes that there are two types of Activity Reports: the audit log Activity Reports and the Sign-ins. [88] Administrators can see the Azure AD activity logs via the Graph API. [89]

The audit log Activity Reports audit log contains the following information:

- Application usage: summary
- Application usage: detailed
- Application dashboard
- Account provisioning errors
- Individual user devices
- Individual user activity

[84] Screenshot published by Microsoft, Audit activity reports in the Azure Active Directory portal, 17 July 2019, URL: https://docs.microsoft.com/en-gb/azure/active-directory/reports-monitoring/concept-audit-logs
[85] Microsoft, Azure AD reporting Logs and reports: Reports user sign-in activities and system activity information about users and group management, 31 October 2019, URL: https://docs.microsoft.com/en-gb/azure/security/fundamentals/log-audit
[86] Microsoft, Interpret the Azure AD sign-in logs schema in Azure Monitor, 18 april 2019, URL: https://docs.microsoft.com/en-gb/azure/active-directory/reports-monitoring/reference-azure-monitor-sign-ins-log-schema
[87] Microsoft, Interpret the Azure AD audit logs schema in Azure Monitor (preview), 18 april 2019, URL: https://docs.microsoft.com/en-gb/azure/active-directory/reports-monitoring/reference-azure-monitor-audit-log-schema
[88] Microsoft, What are Azure Active Directory reports?, 13 November 2018, URL: https://docs.microsoft.com/en-gb/azure/active-directory/reports-monitoring/overview-reports
[89] Microsoft, How to: Use the Azure AD Graph API, 28 August 2019, URL: https://docs.microsoft.com/en-gb/azure/active-directory/develop/active-directory-graph-api-quickstart

- Groups activity report
- Password reset registration activity report
- Password reset activity[90]

Government organisations administrators can view the activities of users through a filtered view.

According to Microsoft, the Sign-in activity reports contain answers to questions such as:

- What is the sign-in pattern of a user?
- How many users have users signed in over a week?
- What is the status of these sign-ins? [91]

These are large files. Microsoft explains: "*Every audit log event uses about 2 KB of data storage. Sign in event logs are about 4 KB of data storage. For a tenant with 100,000 users, which would incur about 1.5 million events per day, you would need about 3 GB of data storage per day. Because writes occur in approximately five-minute batches, you can anticipate approximately 9,000 write operations per month.*"[92]

If an organisation has 1.000 employees, Microsoft describes the organisation will have 15.000 audit events per day, requiring a storage capacity of 900 MB per month, and 34.800 sign-in event per day, with a required storage capacity of 4 GB per month.[93]

Microsoft explains that it collects these data not only for its customers, but also for itself, in order to analyse system usage and improve service. Microsoft says that it, also with this category of data, firstly deletes personal data before processing the data for its own purposes.

Microsoft writes: "*Usage data are metadata generated by the Azure AD service that indicates how the service is used. This metadata is used to generate reports for both administrators and users. It's also used by the Azure AD engineering team to evaluate system usage and identify opportunities to improve the service. This data is generally written to log files, but in some cases it is collected directly by our service monitoring and reporting systems. Personal information is deleted from Microsoft's usage data before it leaves the original environment*."[94]

The deletion (erasure or destruction) of identifying information after its collection is personal data processing. This is subject to the GDPR. The fact that Microsoft deletes certain personal data from the log files, does not make any difference to the assessment that Microsoft processes personal data through these log files. The process of anonymisation and pseudonymisation is further explained in Section 3.2 of this report.

[90] Idem.
[91] Microsoft, What are Azure Active Directory reports?, 13 November 2018, URL: https://docs.microsoft.com/en-gb/azure/active-directory/reports-monitoring/overview-reports
[92] Microsoft, Azure AD activity logs in Azure Monitor, 22 April 2019, URL: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-activity-logs-azure-monitor
[93] Idem.
[94] Microsoft, What are Azure Active Directory reports?

2.5 Data subjects

Via Intune, government organisations process the personal data of employees. Microsoft also processes data about the behaviour of the system administrators of government organisations. Intune and the Azure AD do not process any data about other data subjects, about whom government organisations may process data (in communication with, or files about citizens).

Even if government organisations were to use, for example, Windows Defender or an external supplier of software against viruses and malware, it is unlikely that government organisations would use Intune to process other data about data subjects other than employees. The processing of data via this type of software was not tested for this DPIA. However, it is likely that Intune will only process the compliance status of the devices and possibly enforce the use of antivirus software, but not process content that is scanned via the software.

3. Data Processing

This section describes the privacy choices that system administrators and data subjects (government employees) can make with regard to the diagnostic data collected by Microsoft through the different Intune and AD log files and through the telemetry sent by the Company Portal App. This section also discusses the processing of data that consists of anonymisation. The various technical ways in which Microsoft collects and further processes diagnostic data are further explained in Section 8 of this report (*Techniques and methods of the data processing*).

3.1 Privacy choices Intune and Azure AD

As explained in Section 1.1, under the heading *Outside the scope of this DPIA*, this DPIA is limited to an assessment of the risks for self-managed devices. On Android devices, the least intrusive option was tested, per-application management instead of a strict separation of the device between the personal environment and the work environment (see also Figure 3 in this report).

Microsoft provides a general overview of the different settings system administrators can choose with regard to the management of devices. Depending on the type of enrolment, such options may lead to highly privacy intrusive data processing, such as for example the option to silently turn on screen observation in the Classroom app.[95] It is up to the individual government organisations to determine in a specific DPIA about their Intune deployment what type of monitoring data are necessary to enforce compliance with the their information security policy, while balancing this against the obligation to minimise data protection risks for the employees.

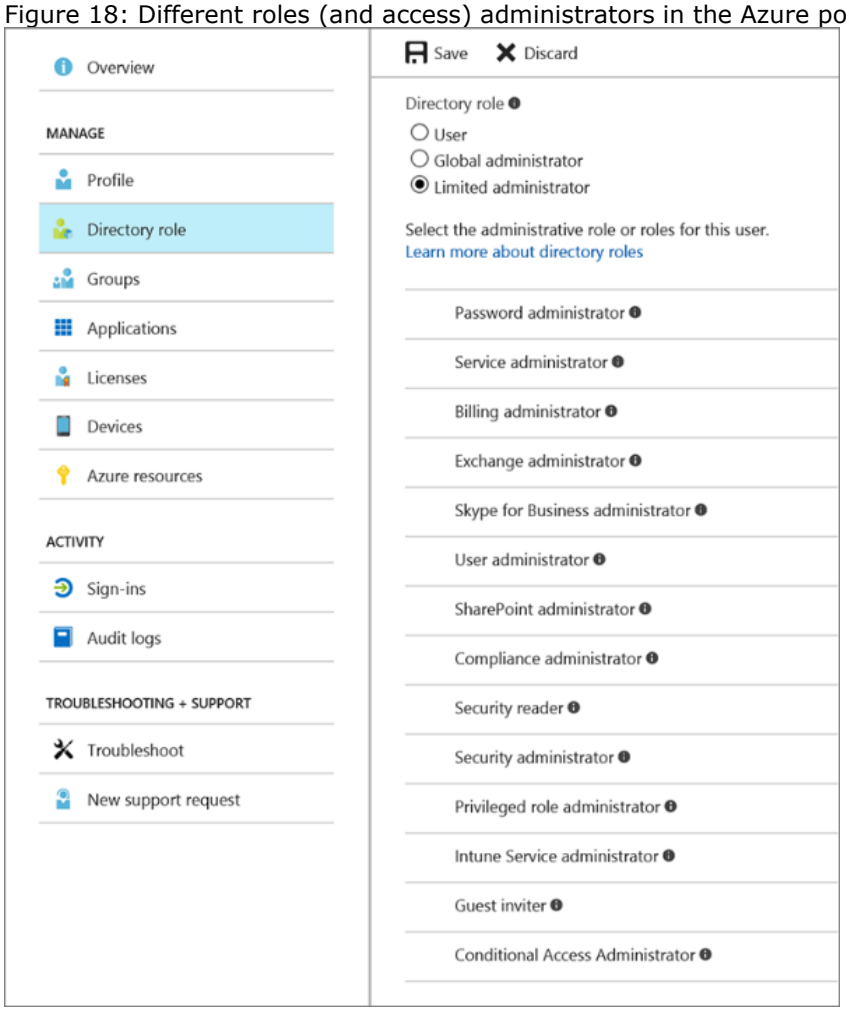
3.1.1 Privacy choices system administrators Intune

Azure AD Privileged Identity Management allows government organisations to keep log files of the system administrators' activities in Intune: the login history, changes to management tasks, and alerts on access to privileged roles. With this management tool, roles such as Global Administrator, Billing Administrator,

[95] Microsoft explains: "*Unprompted screen observation by Classroom app: If set to Allow, teachers can silently observe the screen of students iOS/iPadOS devices using the Classroom app without the students' knowledge. Student devices enrolled in a class using the Classroom app automatically give permission to that course's teacher. Not configured (default) prevents this feature.*"

Service Administrator, User Administrator and Password Administrator can be assigned.

Figure 18: Different roles (and access) administrators in the Azure portal[96]



Changing the status of a device

Although this DPIA is focussed on the use of Intune for self-managed devices, administrators can change the status of devices from personal to corporate. Microsoft explains: *"As an Intune admin, you can identify devices as corporate-owned to refine management and identification. Intune can perform additional management tasks and collect additional information such as the full phone number and an inventory of apps from corporate-owned devices."*[97] Even though Microsoft explains that Intune never collects information from personal devices about apps that are not managed through Intune, Intune does collect information from corporate owned devices about all apps, "*whether those apps are managed or not."*[98] Microsoft explains that it can take up to seven days after the status change before the administrator can see all apps: "*Generally, the report is*

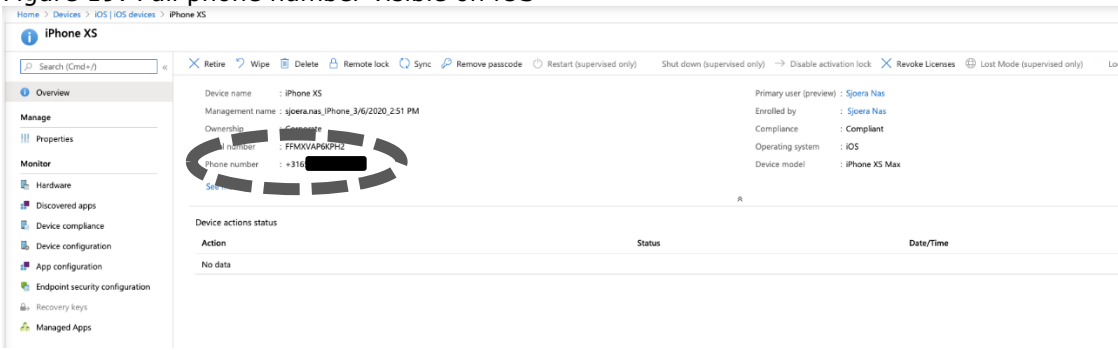
[96] Screenshot provided by Microsoft, Steps to set up Intune, Give admin permissions in the Azure portal, 28 February 2018, URL: https://docs.microsoft.com/en-us/intune/fundamentals/users-add
[97] Microsoft, Identify devices as corporate owned, 22 February 2018, URL: https://docs.microsoft.com/en-gb/intune/enrollment/corporate-identifiers-add
[98] Microsoft, Intune discovered apps, 22 October 2019, URL: https://docs.microsoft.com/en-GB/intune/apps/app-discovered-apps

renewed every seven days from the time of registration (so there is no weekly renewal for the entire tenant)."[99]
The technical research shows that after the status change on iOS, macOS, Android and Windows devices, the system administrators are able to see all installed apps, including private apps that are not managed by government organisations, and the employee's full phone number. The research also shows that the status change does not enable the administrator to see the location data of an iOS device.

As explained in Section 1.2.2 under iOS and macOS, an iOS device can only be set to *fully managed* when it is first issued, not afterwards.

After the status change, on iOS devices the full phone number becomes visible (Figure 19, phone number blacked out in this public report). After the status change on iOS, macOS and Windows 10, the administrator can see all installed apps (Figures 20 and 21). In this test, on iOS apps were included related to health (from health insurance company VGZ and training program 30 Day Fitness) and to video on demand (Netflix). On the macOS device some communication apps were installed (Slack and Teams) and several Microsoft Office apps.

Figure 19: Full phone number visible on iOS



[99] Idem.

Figure 20: All installed apps visible on iOS [March 2020]

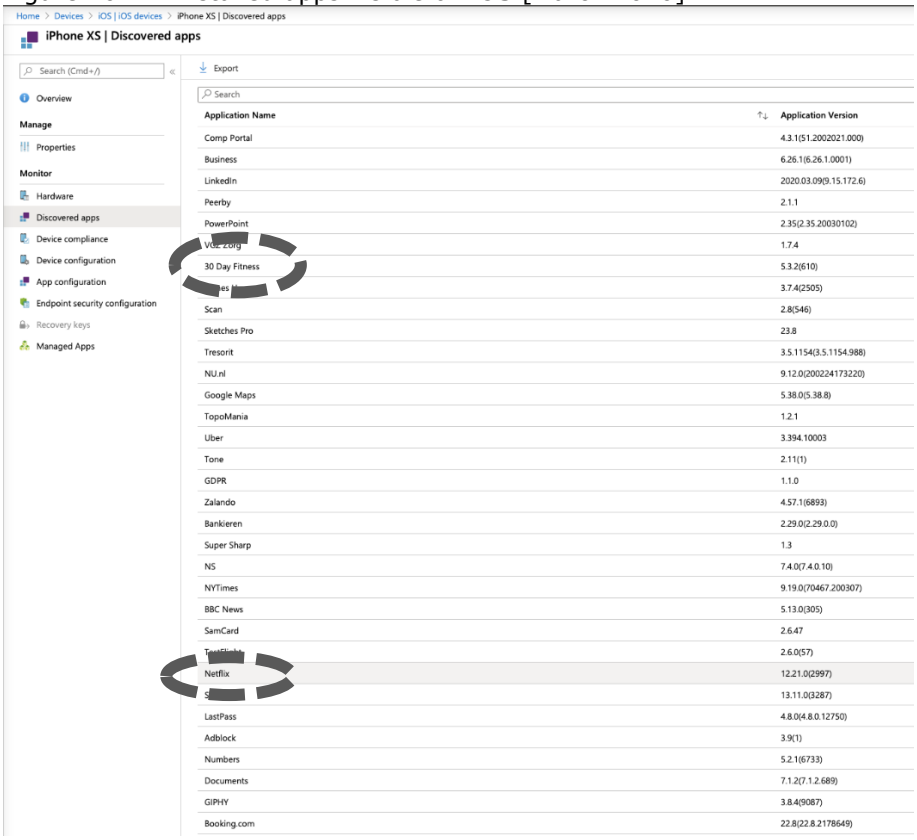
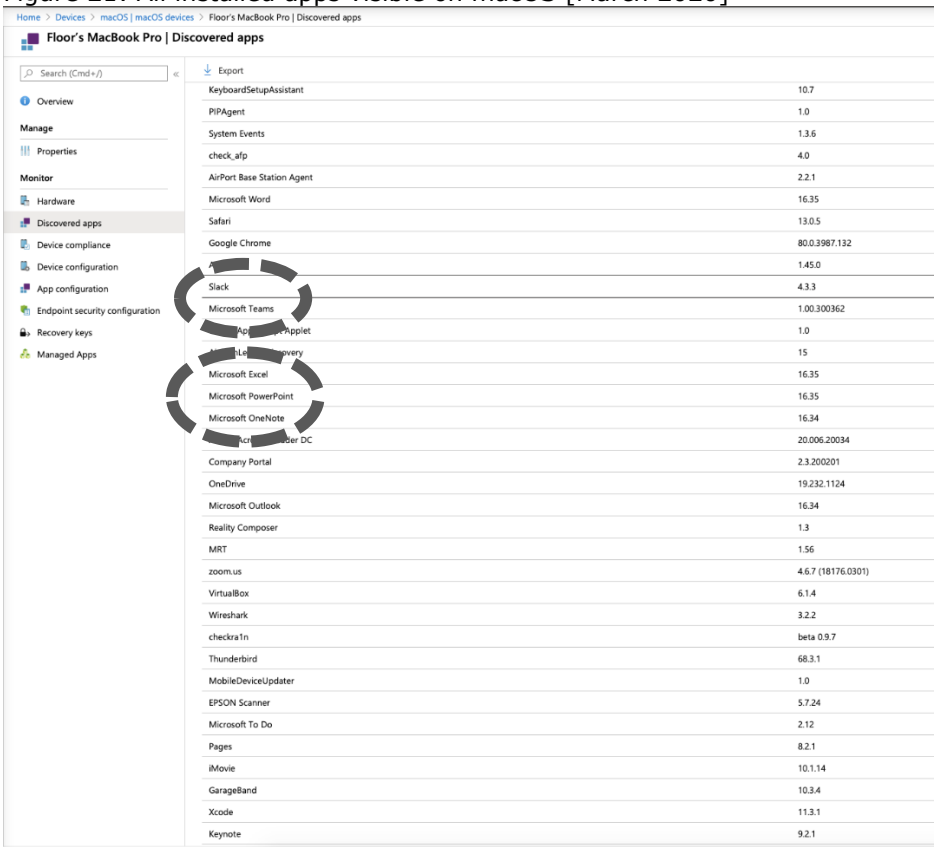


Figure 21: All installed apps visible on macOS [March 2020]



After the status change on Android, the administrator can equally see all installed apps, but not the phone number (Figures 22 and 23). In this example, apps are included from for example Centerparks, Thuisbezorgd and RTL XL.

Figure 22: Phone number not visible on Android

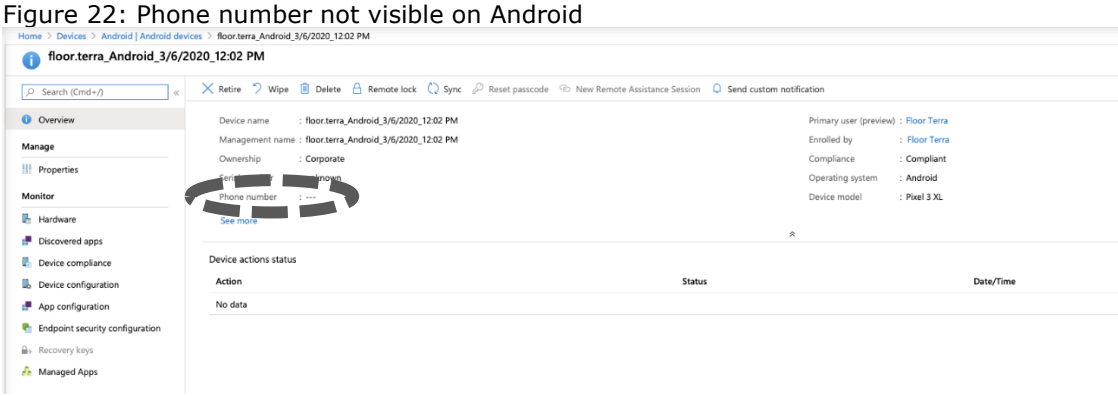
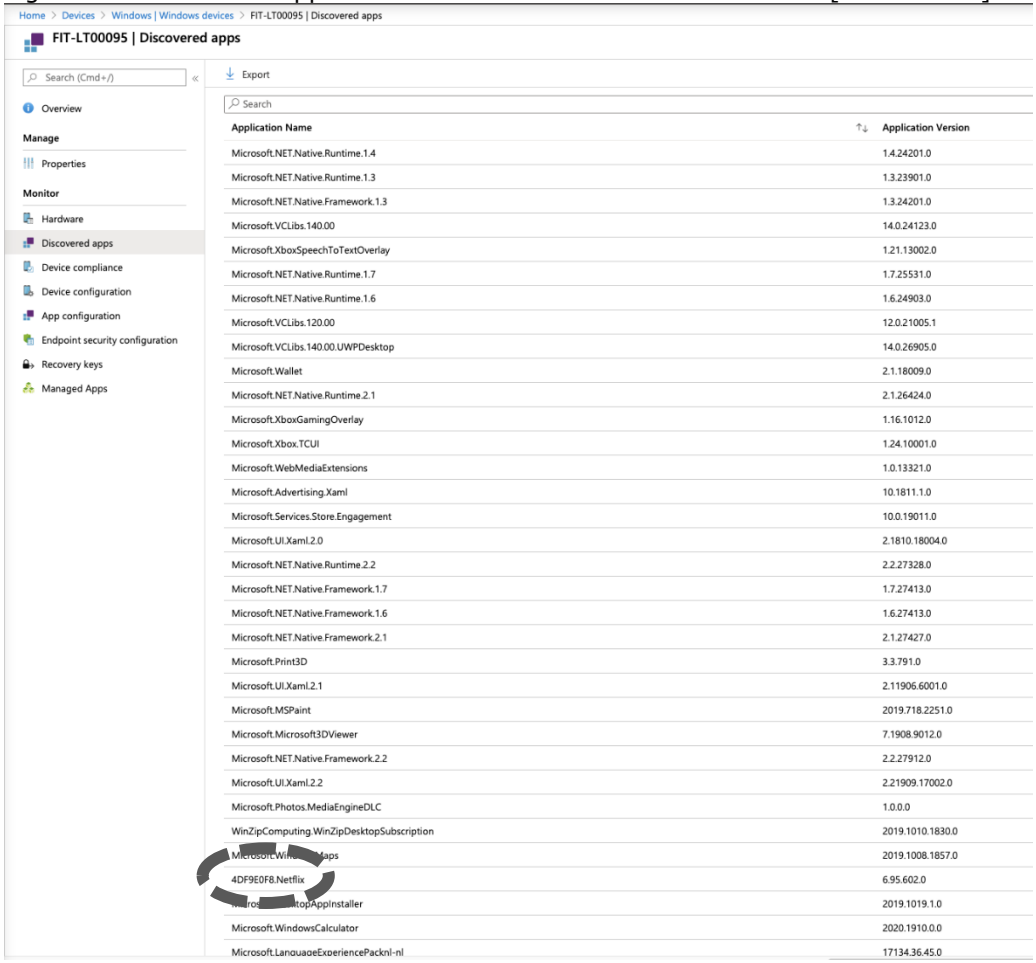


Figure 23: All installed apps visible on Android [March 2020]

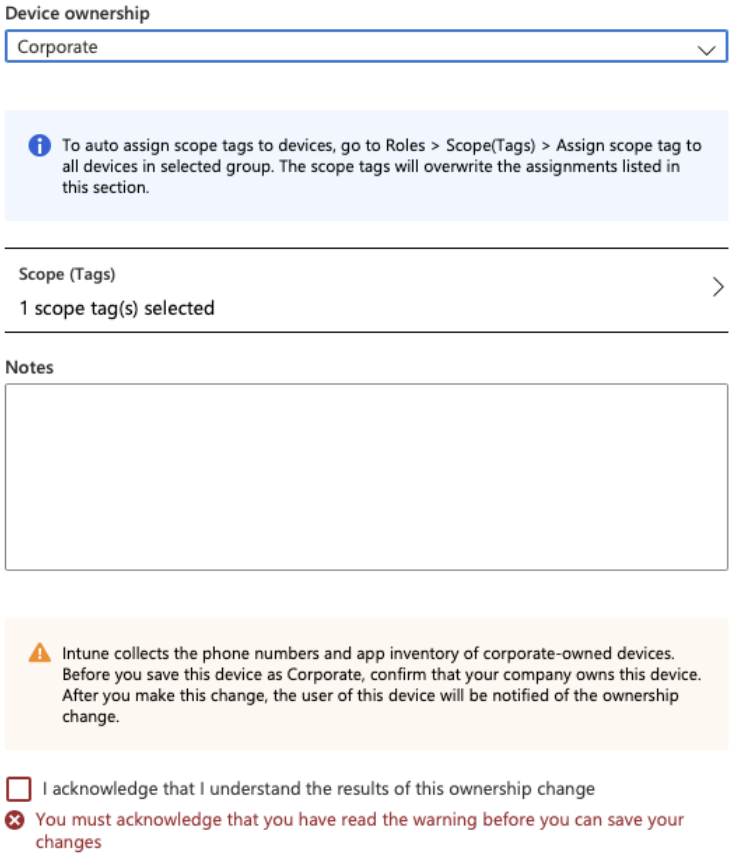
After a status change of a laptop or desktop running Windows 10, the administrator can see all apps that are installed via the Microsoft store, but not any apps that users have installed in different ways, such as for example browsers. See Figure 24.

Figure 24: All installed apps from Microsoft Store visible on Windows [March 2020]



The administrators are not able to see what users do with these apps or which data these apps process.

Figure 25: example Microsoft on converting the management status of the device[100]



When making this change, as shown in Figure 25 above, the administrator will be warned that the user of the device will be informed of the change.

No Data Viewer Tool

As described in Section 2.3, there is no Data Viewer Tool to inspect the telemetry data from the Company Portal App on the different platforms. The system administrators do not have access to the telemetry data from the devices. The only way to obtain information about the contents of both logs is to intercept the outgoing data traffic. This can only be done for iOS devices, as traffic from Android and macOS is protected against interception with certificate pinning, and the telemetry traffic from Windows 10 Enterprise devices is inextricably mixed with the general Windows 10 telemetry traffic (no separate Company Portal app required).

No central blocking option for telemetry and debug logs

During the tests in September/October 2019, there was no possibility for the system administrators to centrally turn off the collection of the telemetry data and the debug log by Microsoft. [101]

[100] Idem.

[101] Microsoft has not yet updated the information from September 2017 on the pages about turning off the collection of data via the Company Portal app on Android and iOS: "*Your company support does not have control over the collection of this data, and they cannot change your selection for the setting*." See for example: URL: https://docs.microsoft.com/en-gb/intune-user-help/turn-off-microsoft-usage-data-collection-ios

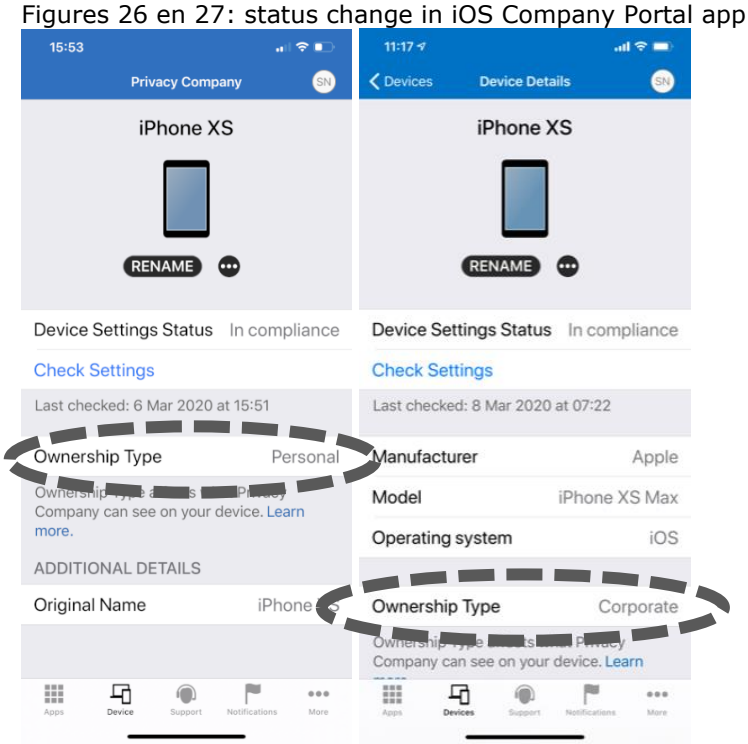
According to updated information published in February 2020, Microsoft now allows administrators in all enrolment types to create the policy 'Block' to prevent iOS and iPadOS devices from sending usage data to Microsoft.[102] For Android, there only is a possibility for Samsung Knox, no such option for Android with Work Profile.[103] No option is documented either for macOS.[104]

Privacy Company changed the settings during the first tests to disable data sharing, and verified that indeed no telemetry data are sent to Microsoft from iOS, macOS and Android if the end-user turned off Usage Data sharing. Although it was not possible to decrypt the telemetry data stream via Android, the tests confirm that the use of the opt-out was effective because no more data were sent to Microsoft's own domain for telemetry (mobile.pipe.aria.microsoft.com) or the external domain gate.hockeyapp.net. On a laptop with Windows 10 Enterprise, the telemetry setting was set to the lowest user-adjustable Basic level. With the help of the Data Viewer Tool, it was determined that Windows does not send any Intune related telemetry data at this telemetry level.

3.1.2 *Privacy choices system end-users Intune*

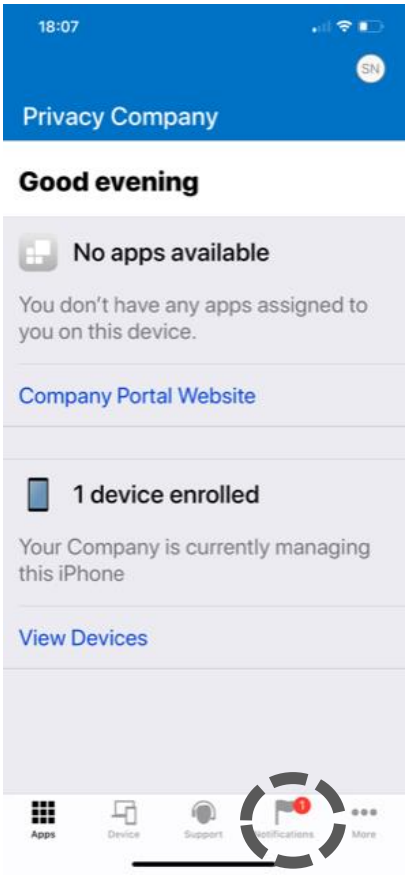
When an employee installs the Company Portal app, no choice is presented or required with regard to the diagnostic data Microsoft will process through the telemetry or through the debug log.

Figures 26 en 27: status change in iOS Company Portal app



[102] Idem.
[103] Diagnostic data submission (Samsung Knox only): Choose Block to stop the user from submitting bug reports from the device. Not configured allows the user to submit the data.
[104] Microsoft, macOS device feature settings in Intune, 18 February 2020, URL: https://docs.microsoft.com/en-gb/intune/configuration/macos-device-features-settings

Figure 28: warning of status change with red flag



When an administrator changes the device status, the employee will only receive a signal of such a change via the Intune Company Portal app itself. This message is only visible when the user of the device opens the Company Portal app and checks the status of the device.

In the Company Portal app, a new notification is also visible on a separate tab, indicated with a red flag. This tab describes the change of ownership type. However, after installation, the user has no reason to open the Company Portal app, so the chance that the user will actually be 'informed about the change of the owner', as Microsoft writes, is negligible.

As explained in Section 2.3 of this report (*Data processed by Microsoft through the Company Portal app*), the use of the Company Portal app leads to the processing of two types of diagnostic data: (1) the telemetry flow to Microsoft and (2) the creation on the device and -user approved- sending of a debug log. Users (the employees of government organisations) can disable both data streams.

Employees with iOS and Android devices can turn off the collection of telemetry data by Microsoft. This can be done on Android in the Company Portal app itself, on iOS in the Company Portal app menu.[105]

- **Android** - via the **Usage data** setting in the Company Portal app.
- **iOS** - via its own Apple main menu with general settings, Company Portal and disable Usage Data. [106]
- **macOS** - Open the Company Portal menu: Preferences, disable consent for collecting usage data by Microsoft.[107]
- **Windows 10 Enterprise** – as verified on 23 October 2019 if users set the telemetry level in Windows 10 Enterprise to "Basic" or "Security", no Intune related telemetry data will be sent via the (restricted) Windows telemetry.

Microsoft also collects a debug log file with extensive details via the Company Portal app by default.[108] Users can choose to disable this more extensive logging of their activities.

[105] Microsoft, How to turn off Microsoft data collection on iOS, 19 September 2017, URL: https://docs.microsoft.com/en-gb/intune-user-help/turn-off-microsoft-usage-data-collection-ios.
[106] Microsoft, iOS and iPadOS device settings to allow or restrict features using Intune, 18 February 2020, URL: https://docs.microsoft.com/en-gb/intune/configuration/device-restrictions-ios
[107] Idem.
[108] Microsoft, Configure logging settings, URL: https://docs.microsoft.com/en-gb/intune-user-help/send-logs-to-your-it-admin-by-email-android Microsoft writes: "*If you experience a problem in the Company Portal or Microsoft Intune app, you can email the*

- **Android** - via Settings in the Company portal app 'Extended logging'[109] Microsoft writes about this: "*The actual error details are kept on your device in a special document called a diagnostic log. When you upload the logs to the Company Portal or Microsoft Intune app, they're first sent to the Microsoft developers that work on the app. They use the logs to improve the app's functionality and prevent future errors. An incident ID for your specific error is then provided to you to share with your company support person, for use in Microsoft Support cases.*" [110]
- **iOS** - via the Apple General Settings main menu, under Privacy, Analytics, Analytics data. Microsoft explains: "*This is a list of app activities that have happened, ranging from crashes to general usage patterns, and it does not contain any personal information.*" [111]

It was verified on 17 October 2019 that it is possible to turn off this form of logging on the device.

3.1.3 Logging choices via the Azure AD

As described in Section 2.4 (*Azure AD Log Files*), Microsoft collects two types of files through the Azure AD: user-defined log files and user-data log files.
A sign in log in the Azure AD contains the following information by Microsoft default:

- The sign-in date
- The related user
- The application the user has signed in to
- The sign-in status
- The status of the risk detection
- The status of the multi-factor authentication (MFA) requirement[112]

Administrators can add the following data to this information:

- Username
- IP address
- App
- Operating system
- Device browser
- Location
- Correlation ID
- MFA Authentication method
- MFA Authentication detail
- MFA Result[113]

---

details of the problem to your company support person. These details will provide them with additional context about the problem.
The actual error details are kept on your device in a special document called a diagnostic log. When you upload the logs to the Company Portal or Microsoft Intune app, they're first sent to the Microsoft developers that work on the app. They use the logs to improve the app's functionality and prevent future errors. An incident ID for your specific error is then provided to you to share with your company support person, for use in Microsoft Support cases."
[109] Idem.
[110] Idem.
[111] Microsoft, Send logs to the Company Portal developers for iOS devices, URL: https://docs.microsoft.com/en-gb/intune-user-help/send-logs-to-microsoft-ios
[112] https://docs.microsoft.com/en-gb/azure/active-directory/reports-monitoring/concept-sign-ins
[113] Idem.

3.2 Anonymisation and pseudonymisation

Microsoft explains that it automatically collects certain data via the Company Portal app and that it anonymises these data. Microsoft does not publish any explanation as to what it understands by anonymisation in this case. In the improved privacy terms negotiated by SLM Rijk, Microsoft guarantees application of the anonymisation standards defined by the European data protection authorities in Opinion WP216.[114]

Microsoft also describes that the Azure AD log files contain usernames, but that it removes those personal data from the log files (scrubbing) before processing the data in its machine learning systems for general analysis.

Anonymisation is a complex and dynamic form of data processing. Often organisations still have original data in other databases or continue to collect new pseudonyms. As long as there is a realistic possibility of re-identifying the pseudonymised data, the stored data cannot be considered anonymous and Microsoft, and government organisations as joint data controllers via the app, still need a legal basis for the collection of the personal data and the purpose of the anonymisation. Indeed, under Article 4(5) of the GDPR, the processing of pseudonymised data is still processing of personal data.

Even if the stored data have been made technically irreversibly anonymous (instead of hashed or encrypted, or stripped from directly identifying data such as e-mail addresses), the GDPR rules apply from the start of processing when the data are collected from an identifiable end user and sent to Microsoft. The deletion (anonymisation, deletion or destruction) of identifying data after its collection is in fact also a processing of personal data. This processing is also subject to the GDPR. Therefore, the fact that Microsoft deleted certain personal data from the log files does not make any difference in the assessment that Microsoft processes personal data through these log files.
It is quite conceivable that Microsoft, as a 100% part of Azure, processes and stores the Intune log files in the same way as the data from Office 365, namely in the central Cosmos database. The unique user identifiers from the audit logs are replaced by hashes, but the service teams can undo this form of pseudonymisation.

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

[114] Article 29 Working Party, WP126, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Contracts with Cosmos, and the controls that Office 365 inherits directly from Cosmos were directly assessed by the third-party assessment organization." [115]

The detailed notes in the NIST document state that the only change Microsoft makes to the audit logs before these logs are sent to Cosmos is the replacement of directly identifiable personal data by hash values. "*It was also noted that no data leaving the Office 365 boundary (Cosmos is located outside the boundary) can leave in clear text. Thus, the only modification made to audit records being sent to Cosmos is part of the scrubbing process which includes replacing all personally-identifiable information (PII) with a hash value. (…) It was determined that once the PII is encrypted, the PII can be decrypted only by a user with the proper decryption key. Therefore, it was determined that provides an audit reduction capability that does not alter the original content or time ordering of audit records*." [116]

If Microsoft applies a similar technique to the diagnostic data from Intune and the Company Portal app, this processing cannot be considered as a form of anonymisation. However, these are good technological measures to protect the confidentiality of the data. Since anonymisation is highly dependent on the actual circumstances of the processing, any statement about anonymisation must be technically verified.

4. Purposes of the processing

Government organisations may want to use Intune for several purposes. The interests of government organisations in using Intune are set out in Section 6 of this report (*Interests in data processing*). Government organisations have their own specific purposes for the processing of diagnostic data from Intune in order to be able to register, encrypt and delete (part of) the self-managed devices and to restrict access to (personal) data via Microsoft apps.
However, Microsoft also determines a number of purposes for the data processing, both in terms of the diagnostic data it collects itself about the use of Intune, the Azure Ad and the Company Portal app, as well as the data that it provides by default to the administrators.

Below are the different purposes discussed for which Microsoft - until now - allows itself to process data contractually.

1. Purposes for processing the diagnostic data from Intune MDM and MAM
2. Purposes for processing the telemetry data and debug log from the Company Portal app
3. Purposes for processing Azure AD diagnostic data

But first the consequences of the improvement of the privacy conditions with Microsoft will be explained.

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

4.1 Limitation to three purposes for cloud services

Thanks to the improved privacy conditions with SLM Rijk, Microsoft may only process the data from Intune MAM and MDM for the following three purposes, and only when proportionate:

1. providing and technically improving the service
2. keeping the service up to date and
3. secure.

This strict purpose limitation does not only apply to the content of customer data, but also to all types of diagnostic data, including telemetry messages from installed software and apps, and the system-generated event logs on Microsoft's own servers.

As explained above, Microsoft already promises in the OST that it will not use the customer data content of any core online services, including Intune, for advertising or marketing purposes: "*Microsoft will not use or otherwise process or derive any information from any Customer Data for any advertising or similar commercial purposes*." This restriction was further tightened by SLM Rijk. In the privacy amendment, Microsoft guarantees that it will never use either the content data or other personal data (including diagnostic data) for profiling, data analytics, market research or advertising, unless the customer explicitly requests it.[117]

In addition, the improved privacy terms contain an exhaustive list of purposes for which Microsoft may process data as an independent data controller, to the extent that this is necessary for its business operations, in order to be able to provide the services as a data processor. These purposes vary from self-evident (sending invoices to customers, producing statistics for the annual financial reports) to purposes that are often overlooked, such as complying with the orders of the law enforcement and security services. This purpose is explained separately in Section 4.4 of this report (Disclosure to law enforcement and security services).

4.2 Purposes Company Portal app

As explained in Section 1.4 of this report (*Privacy Amendment SLM Rijk*), the processing of personal data associated with the Company Portal app falls within the scope of the OST and privacy amendment.

However, Sections 1.4.1 and 1.4.2 of this report describe two circumstances that make it likely that Microsoft considers itself data controller for these diagnostic data, instead of data processor. In its general privacy statement (most recently amended in February 2020), Microsoft describes these purposes as controller as follows: "*We also use the data to operate our business, which includes analysing our performance, meeting our legal obligations, developing our workforce and doing research.*"[118]
According to its privacy statement, Microsoft can process data for 17 purposes. This includes the display of personalised advertising and the use of the data for any purpose that Microsoft deems compatible with the provision of the services.[119]

[117] See also sections 4.1 of the two DPIAs published in the summer of 2019 about Office 365 ProPlus and Office Online and the mobile Office apps, on the website of SLM Rijk.
[118] Microsoft privacy statement, last updated February 2020, URL: https://privacy.microsoft.com/en-gb/privacystatement See: 'How we use personal data'.
[119] Also see section 4 of the umbrella-DPIA report on Office ProPlus for SLM Rijk. In July 2019 Microsoft had twelve purposes for the processing of telemetry data, based on its then-valid general privacy statement.

1. Provide our products
2. Product improvement
3. Personalisation
4. Product activation
5. Product development
6. Customer support
7. Help secure and troubleshoot
8. Safety
9. Updates
10. Promotional communications
11. Relevant offers
12. Advertising
13. Transacting commerce
14. Reporting and business operations
15. Protecting rights and property
16. Legal compliance
17. Research[120]

Microsoft repeats several times on information pages about the Company Portal app that it does not sell data collected with the services to third parties. Microsoft does not define what it means by "sale," but the warning may be intended to explain why Microsoft is not offering an opt-out of the sale, an obligation under the new Californian Consumer Privacy Act CCPA, which entered into force on January 1, 2020.[121]

Figure 29: Microsoft Notes: No Selling Intune Data to Third Parties (also in Dutch)

Under the heading "Advertising" in the Privacy Statement, Microsoft explains that it "shares" (rather than "sells"): "*We may share data we collect with partners, such as Verizon Media, AppNexus or Facebook (see below), so that the ads you see in our products and their products are more relevant and valuable to you.*"[122]

Microsoft mentions some examples of these types of other companies that may obtain usage information: "*Additionally, Microsoft partners with third-party ad companies to help provide some of our advertising services, and we also allow other third-party ad companies to display advertisements on our sites. These third parties may place cookies on your computer and collect data about your online activities across websites or online services. These companies currently include,*

[120] Microsoft privacy statement, last updated February 2020, list beneath 'More information about the purposes of the processing', URL: https://privacy.microsoft.com/en-GB/privacystatement.
[121] https://iapp.org/resources/article/california-consumer-privacy-act-of-2018/#1798.135
[122] Microsoft privacy statement February 2020.

but are not limited to: AppNexus, Facebook, Media.net, Outbrain, Taboola and Verizon Media."[123]

Microsoft explicitly mentions the possibility that it can base its advertisements on usage data: "*The ads that you see may also be selected based on other information learned about you over time using demographic data, location data, search queries, interests and favourites, usage data from our products and sites, as well as the sites and apps of our advertisers and partners. We refer to these ads as "personalised advertising" in this statement."*[124]

In response to the applicability of the conditions of the general consumer privacy statement to the data processing via the mobile Office apps, Microsoft replied to SLM Rijk that all data collected through the use of an Azure work account are governed by the negotiated privacy amendment.

"*All Office Mobile applications are (indeed) offered under a EULA between Microsoft and the mobile device user, and the diagnostic data it collects is governed under the Microsoft Privacy Policy and the EULA. However, and crucially, data provided to Microsoft or collected by Microsoft through the use of an Azure AD Account authenticated in the Mobile apps are governed under the OST and your agreement."*[125]

This phrasing however does not include telemetry data that are sent from the app, separate from logged-in activities.

4.3 Purposes Azure AD

Microsoft collects and processes various log files about the Azure AD. Microsoft not only does this for the benefit of its customers, but also for its own purposes.

As mentioned in Section 2.4 of this report (*Azure AD log files*), Microsoft describes that it can also process the log files with usage data (with the activity reports and sign in logs) for its own purposes. In addition, Microsoft collects log files that the customer does not have access to.

Microsoft indicates in its own white paper that it processes the Azure AD log files for six of its own purposes:

1. Auditing
2. Investigation
3. Usage analysis
4. Removing software errors (debugging)
5. Systemic health analysis
6. System-wide analysis with machine learning[126]

Microsoft indicates in this white paper that it collects and processes certain log files only for itself, for its own purposes, and that it does not give its customers access to these *system generated* log files.

"*Microsoft will make logs of events occurring on Microsoft operated infrastructure and solutions as needed to serve our purpose in operating that infrastructure. Azure Activity logs, accessible to the customer, are logs about the use of that*

[123] Ibid.
[124] Ibid.
[125] E-mail Microsoft to SLM Rijk 19 July 2019.
[126] Public Microsoft whitepaper, Ramiro Calderon, Azure Active Directory Data Security Considerations, Version: 1.01, Published: June 2018, URL: https://aka.ms/aaddatawhitepaper.

Customer Data for which Microsoft is a processor (activities in on Azure resources). Other infrastructure level logs (System Generated Logs), usually not accessible or useful to the customer, are part of the detailed means by which we make sure we can operate the Azure services, secure the platform and meet the SLA". [127]

Microsoft published a (public) audit report on Azure (testing against ISO 27001 and 27018).[128] This shows that Microsoft also generates at least one other type of log file for its own purpose of *Operations security*. Under the heading 'Operations Security - Logging and Monitoring and Baseline Management', the audit report explains that Logging Monitoring is a Cloud and company-wide implemented program. The report describes the following approach: - *Data collection - processing and analysis - alerts and response*

In total, Microsoft processes the data on the use of the Azure AD for eight purposes:

1. Auditing
2. Investigation
3. Usage analysis
4. Removing software errors (debugging)
5. Systemic health analysis and
6. System-wide analysis with machine learning
7. Security of the platform
8. Discovering opportunities for product improvement

The auditor notes that Microsoft engineers review the numbers and types of events every six months.

According to the improved privacy conditions negotiated by SLM Rijk Microsoft is limited to 3 purposes for the processing of personal data on the use of the Azure AD, and only to the extent that this is necessary to achieve these purposes.

4.4 Disclosure to law enforcement and security services

If Microsoft is forced to do so by a legal order and a 'gagging order' from law enforcement and security services, Microsoft must provide personal data without being allowed to inform its customer. In its new Data Protection Addendum, Microsoft provides an explicit guarantee with regard to disclosure to all Processed Data, no longer limited to Customer Personal Data.

Processed data are described as follows: "*Processed Data" means: (a) Customer Data; (b) Personal Data; and (c) any other data processed by Microsoft in connection with the Online Service that is Customer's confidential information under the volume license contract. All processing of Processed Data is subject to Microsoft's obligation of confidentiality under the volume license contract.*"[129]

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

[127] Idem.
[128] BSI Assessment report on compliance standard ISO/IEC 27001:2013 and ISO IEC 27018:2014 by Microsoft Azure, published on 23 August 2018, p. 13.
[129] Microsoft Online Services Data Protection Addendum, January 2020, p. 6.

Upon receipt of any other third-party request for Processed Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.[130]

SLM Rijk's improved privacy conditions clarifies that Microsoft will not act as a processor if it is required to comply with an order to disclose personal data (whether it is customer content or diagnostic data) to law enforcement, security or secret services in the United States. In these circumstances, Microsoft acts as a sole controller because, as a company, it must comply with legal obligations imposed upon it under U.S. law. In this situation, Microsoft cannot act as a data processor, because the GDPR legally prohibits customers in the EU from handing over data to services from countries outside the EU in the absence of a mutual legal assistance contract (Article 48 of the GDPR). This does not prejudice the fact that Microsoft should in all circumstances act as data processor, and therefore the law enforcement authority should always refer to the controlling customer.

5. (Joint) controller or processor

5.1 Definitions

The GDPR contains definitions of the various parties involved in the processing of data: (joint) controller, processor and subprocessor.

In Article 4(7), the GDPR defines the (joint) controller as:

> "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*"

Article 26 of the GDPR provides that joint controllers must define their roles and responsibilities, in particular towards data subjects, in a transparent contract.

The GDPR provides in Article 4(8) that a processor may only process data on the instructions of a controller.

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

Article 28 of the GDPR sets out the obligations of processors with regard to the controllers for whom they process data. Article 28 lays down specific obligations for the processor, such as the obligation to process personal data only in accordance with documented instructions from the controller, and the obligation to cooperate, for example, in audits. It follows from Article 28(4) GDPR that a processor may use subprocessors to perform specific tasks for the controller, but only if the same data protection obligations are imposed on that other processor by way of a contract.

[130] Idem.

5.2 Microsoft as processor for Intune MDM and MAM and Azure AD

In the OST, that form part of Microsoft's framework contract with SLM Rijk, Microsoft states that it is a data processor for the processing of data from and about the Intune cloud services and about the Azure AD.

Section 4.3 (*Purposes Azure AD*) explains that Microsoft processes Azure AD usage data for eight purposes, some of which are in Microsoft's best interest. This self-determination of purposes is especially problematic with regard to log files with personal data about employees of government organisations that the organisation do not even have access to. According to the SLM Rijk privacy amendment, Microsoft may in principle only process personal data from the Online Services for three purposes, and only if the processing of data for those purposes is proportionate.

At least 3 of the 8 Azure AD purposes do not seem to fit well in the agreed 3 overall purposes: systemic health analysis, system-wide analysis with machine learning and discovering opportunities for product improvement. To verify Microsoft's compliance with the agreed purposes, SLM Rijk should use its right of audit, as included in the DPA and the privacy amendment, to check that Microsoft no longer processes the data for its own purposes. If Microsoft does not actually act as a processor, the company is in fact a (joint) controller with the government organisations that make these processing operations by Microsoft possible.[131]

5.3 Microsoft as controller for the Company Portal app

Microsoft considers itself to be a (independent) **controller** of the diagnostic data it processes about the use of the Intune Company Portal app, and the data processing via the built-in functionality in Windows 10 Enterprise. As explained in Section 4.2 above (*Purposes Company Portal app*), Microsoft, by virtue of its privacy statement, authorises itself to process the telemetry data and the diagnostic data from the debug logs for seventeen purposes.

Use of the Company Portal app (and similar built-in functionality) is required to register employees' self-managed devices in Intune (except for Windows 10 Enterprise). If government organisations decide to roll out Intune, thereby de facto requiring the use of the Company Portal app, they enable Microsoft to process personal data about the use of this app for its own purposes. Therefore, in practice, government organisations become joint controllers for these data processing operations with Microsoft when they roll out Intune. Section 3.1 explains how employees can disable data sharing with Microsoft. Even though Microsoft recently added an option for administrators to centrally block the sending of usage data in iOS and iPadOS devices, there is no central option to disable this processing on all devices.

Both the public DPIA for SLM Rijk on Microsoft Office apps as well as the public DPIA on Windows 10 Enterprise show that Microsoft (still) considers itself controller for the operating system and installed software. In addition to the ongoing negotiations about Windows 10 Enterprise, the Dutch government should continue to negotiate with Microsoft to ensure that Microsoft correctly applies the

[131] See the caselaw of the European Court of Justice about joint responsibility, in **C-40/17,** 29 juli 2019, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629, **C-210/16**, 5 juni 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein versus Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388. In particular, see: par. 38-43. See: **C-25/17**, 10 July 2018, Tietosuojavaltuutettu versus Jehovah's Witnesses — Religious Community, ECLI:EU:C:2018:551, par. 66-69.

privacy amendment to the processing related to all Online Services (including Intune and the Company Portal app) and to bring all other Enterprise software within the scope of the improved privacy conditions.[132]

6. Interests in the data processing

This section outlines the different interests of Microsoft on the one hand and government organisations on the other. The interests of the Dutch government organisations may align with the interests of its employees. However, this section does not describe the fundamental data protection rights and interests of data subjects. How their rights relate to the interests of Microsoft and the Dutch government organisations is analysed in part B of this DPIA.

6.1 Interests of the Dutch government organisations

Government organisations may want to use Intune for information security and compliance reasons.

As part of their information security policy, government organisations need to encrypt (confidential and/or personal data on the) self-managed devices, and get more control over the devices' access to organisational data. Since Dutch government organisations primarily work with Microsoft products and services, and Intune for MDM and for MAM is included in the Microsoft 365 Enterprise license, the obvious choice is to investigate whether the information security purposes can be achieved with Intune, without causing high data protection rights for the employees.

Government organisations can use Microsoft Intune for two different security purposes, namely (1) enforcing compliance by the devices with the information security policy (MDM) and (2) controlling the access of apps on the devices to the (personal) data (MAM).

Intune MDM allows organisations to centrally register the self-managed devices and encrypt the data on the devices. Government organisations can also check via Intune that employees are not putting their devices into an unsafe mode. Intune MDM can only be used in conjunction with the Azure AD. This identity service is attractive to system administrators because it offers standard support for the oAuth and Saml cloud protocols and because it offers extensive possibilities to add, update and delete users, to register devices and manage the authorisations per user.
Intune MAM allows organisations to control access to (personal) data from specific Microsoft 365 apps, and selectively delete information from managed apps in case of device loss. One of the settings in Intune MAM is that users can only save files from the Office apps in SharePoint Online and OneDrive for Business. This reduces the risk of government organisations losing control over authorisations by storing files on the hard drive or in third-party cloud services.

The use of Intune MDM and MAM thus makes an important contribution to the implementation and monitoring of compliance with the information security policy, including the prevention of personal data breaches (data breaches) as referred to

[132] All DPIA reports are published in English, with a summary in Dutch. See the overview on the website of SLM Rijk), URL: https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise

in article 4(12) of the GDPR.[133] By using adequate, *state-of-the-art* encryption of personal data on the self-managed devices, government organisations **mitigate the risk of reputational damage**. Without such encryption the organisations would have to report any lost device to the Dutch DPA, and in many cases, they would also have to inform all data subjects whose data could be on the device. For an overview of the different types of security risks that government organisations want to prevent with Intune, see also the EDPS guidelines on the protection of personal data on mobile devices.[134]

Last but not least, government organisations may have a financial interest in being able to centrally encrypt self-managed devices. This allows government organisations to let employees buy and manage their own devices. This could reduce the (administration) costs of centralised purchasing and administration of mobile devices.

6.2 Interests of Microsoft

The transition to the cloud is necessary to increase the security of services, according to Microsoft. Microsoft considers it as a vital interest for society, but also as a business and economic interest to be able to process large amounts of data in the cloud, in order to be able to identify and defend against security risks. Local solutions are inevitably more expensive and less effective, according to Microsoft.

Microsoft wants to *be cloud first and mobile first* since 2014.[135] Microsoft explains: "*Our users don't simply use a workstation at a desk to do their jobs anymore. They're using their phone, their tablet, their laptop, and their desktop computer, if they have one. It's evolved into a devices ecosystem rather than a single productivity device (..)*."[136]

Microsoft has a financial and economic interest in selling Intune as an additional management and security service on a license basis, as part of a Microsoft 365 package license, or in addition to a separate Office 365 license. Microsoft has a strong financial and economic interest in providing a (monthly or annual) subscription service. Microsoft has been fundamentally changing its business model for many years: from a software vendor to a monthly subscription service vendor.
The purposes of processing the diagnostic data from the Company Portal app show that Microsoft has its own commercial interests in processing personal data to develop new services, or to discover patterns based on *machine learning*. Although Microsoft indicates in the explanation of the Company Portal app that it does not *sell* data about the use of the app to third parties, this promise does not preclude the *sharing* of such data with third parties, and its use for its own marketing and advertising purposes.

As explained in Section 4.1 of this report (*Limitation to 3 purposes for cloud services*), the Dutch government's privacy amendment stipulates that Microsoft may never use personal information from or about the use of the online services

[133] Article 4(12) GDPR: "**personal data breach**' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"
[134] EDPS, EDPS Guidelines on the protection of personal data in mobile devices used by European institutions, December 2015, URL: https://edps.europa.eu/sites/edp/files/publication/15-12-17_mobile_devices_en.pdf
[135] Microsoft blog, Cloud-first, mobile-first: Microsoft moves to a fully wireless network, August 17, 2016, URL: https://azure.microsoft.com/en-gb/blog/cloud-first-mobile-first-microsoft-moves-to-a-fully-wireless-network/.
[136] Idem.

for marketing or profiling purposes. However, this privacy guarantee does not apply to the telemetry data from the Company Portal app. Therefore, government organisations cannot exclude that Microsoft, for example, collects information about the nature of the mobile device and versions of the operating system used, and uses that input for targeted in-app advertisements.

6.3 Shared interests

The interests of Microsoft and government organisations are aligned when it comes to the use of a limited set of diagnostic data to provide a properly functioning service that allows government organisations to control access to (personal) data on devices and in apps. As part of the shared security interest, it is also appropriate for Microsoft to keep log files on the activities of the system administrators, and to provide technical updates to the Intune service and the Company Portal app. Section 8 (*Legal and policy framework: ePrivacy Regulation*) sets out the requirements of the upcoming ePrivacy Regulation. This shows that the updates must not disrupt the service and that the technical managers must be able to adjust the updates.

In sum, Microsoft has financial, economic and commercial/business interests in collecting diagnostic data. Some interests are in line with the interests of government organisations, while others are not.

7. Transfer of personal data outside of the EU

Articles 44 to 49 GDPR lay down rules for the transfer of personal data to countries outside the European Economic Area (the EU member states and Iceland, Liechtenstein and Norway). In principle, personal data may only be transferred to countries outside the EEA if the country has an adequate level of protection. Such adequacy can be determined in a number of ways.

The European Commission can take a so-called adequacy decision. This means that the country in question has a level of protection comparable to that applied within the EEA. In addition, the EU and the U.S. have made separate contracts about the level of protection of personal data. Through the Privacy Shield (formerly: Safe Harbour) US American undertakings can self-certify as to their standard of protection of personal data. In that case, data controllers in the EU may transfer personal data to such a company.

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

7.1 Intune cloud services

Sections 2.2.1 and 2.2.2 of this report describe the diagnostic data that Microsoft generates in log files on its own servers about the use of Intune MDM and Intune MAM. The SCC apply to the transfer of these personal data from the core online services such as the cloud elements of Intune (for which Microsoft is the processor).

Microsoft describes the storage locations as follows:
"All non-telemetry data collected is processed through the Intune service and is stored in one or more of the following storage locations:

- *SQLAzure*
- *Reliable Collections (Service fabric)*
- *Azure storage"*[137]

Microsoft publishes a list of network endpoints and IP addresses for the cloud service Microsoft Intune.[138] Almost all of these domains end in .manage.microsoft.com. In addition, Microsoft sends functional traffic to login.microsoftonline.com, to config.office.com and graph.windows.net. A number of these network endpoints were observed in the app's network traffic, as well as other traffic. This telemetry traffic is discussed in Section 7.2 below.

As briefly mentioned in Section 1.4 (*Privacy amendment SLM Rijk*), Microsoft guarantees via the OST that the subcategory of content data of the Core Online Services, which Microsoft defines as Customer Data, will only be stored in data centers in the EU. About the Microsoft Intune Online Services, Microsoft writes in the OST: "*For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as set forth in Attachment 1 to the OST."*[139]

In Attachment 1 to the OST (with the table of Core and Other Online Services) Microsoft adds the following information: "*Microsoft Intune Online Services. When Customer provisions a Microsoft Intune tenant account to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo except as noted in the Microsoft Intune Trust Center."*[140]

Microsoft explains in the Trust Center, with a map of Europe, that it processes the Intune cloud data content in data centres in Ireland and the Netherlands if the customer is based in Western Europe.[141]

Legally, the guarantees Microsoft offers via the OST only apply to the Customer Data, and only to the extent that they are stored (data at rest). Microsoft therefore does not give guarantees for the data in transit, nor for the diagnostic data. The contents of data generated and received by government organisations may be routed through other locations during the transfer and may also be processed in other regions. Microsoft has explained that processing can take place at any location where Microsoft operates (except in China, as this is a completely separate cloud). With regard to the Azure AD log files, Microsoft does make a promise about the location of the primary processing, but ultimately those log files will also be stored in the U.S. See Section 7.3 (*Azure AD*) below.

Even if Microsoft were to store all data from and about the Intune cloud service, including the diagnostic data, only in data centres in Europe, Microsoft could still receive an order from U.S. law enforcement authorities to grant access to those personal data. The USA CLOUD Act extends the jurisdiction of North American courts to all data under the control of U.S. companies, even if that data are stored in data centres within the EU, outside the territory of the U.S.

The European Data Protection Committee and the EDPS have issued opinions on the CLOUD Act to the LIBE Committee of the European Parliament. They explain

[137] Microsoft, Data storage and processing in Intune, 18 May 2018, URL: https://docs.microsoft.com/en-gb/intune/protect/privacy-data-store-process
[138] Microsoft, Network endpoints for Microsoft Intune, 22 July 2019, URL: https://docs.microsoft.com/en-us/intune/fundamentals/intune-endpoints
[139] Microsoft OST, March 2020.
[140] Idem, Attachment 1, p. 27.
[141] Microsoft Intune datacenter map, URL: http://intunedatacentermap.azurewebsites.net/

that transfers of personal data from the EU have to comply with Articles 6 (basis for processing) and 49 (exceptions allowing for transfers) GDPR. If an order is issued on the basis of the CLOUD Act, the transfer can in principle only be lawful if there is an international treaty between the EU and the U.S. So far, this is not the case. Only the United Kingdom has recently concluded a separate contract with the U.S.[142]

The Data Protection Authorities write: "*unless a U.S. CLOUD Act warrant is recognised or made enforceable on the basis of an international contract, and therefore can be recognised as a legal obligation, as per Article 6(1)(c) GDPR, the lawfulness of such processing cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject on the basis of Article 6(1)(d) read in conjunction with Article 49(1)(f).*"[143]

In their accompanying letter, the data protection authorities stress the urgent need to conclude a new generation of Mutual Legal Assistance Treaties, which should ensure much faster and safer processing of mutual assistance requests in practice. " *In order to provide a much better level of data protection, such updated MLATs should contain relevant and strong data protection safeguards such as, for example, guarantees based on the principles of proportionality and data minimisation. In addition, the "dual criminality principle" providing safeguard against discrepancy between how a crime is defined under the foreign law and how the same crime is legally defined under EU law should be preserved.*"[144] The DPAs also refer to the ongoing negotiations on an international EU-U.S. convention on cross-border access to electronic evidence for judicial cooperation in criminal matters.[145]

7.2 Intune Company Portal app

Section 2.3 of this report (*Data processed by Microsoft through the Company Portal app*) describes the telemetry data that Microsoft collects via the Intune Company Portal app.

As explained in Section 1.3 (*Framework contract with SLM Rijk*), Microsoft had a large number of audits performed on its core online services, including Intune. These include identity and access management via Intune and the Azure AD, but do not cover the diagnostic data that Microsoft collects via the Company Portal app, the similar built-in Intune functionality of Windows 10 Enterprise, or the debug logs.

[142] USA department of justice, press release about the agreement with the U.K., 3 October 2019, URL https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists#targetText=The%20Agreement%20was%20facilitated%20by,related%20review%20by%20UK's%20Parliament.

[143] Annex EDPB and EDPS joint response to U.S. CLOUD Act, 10 July 2019, p. 8. URL: https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[144] Idem, accompanying letter 10 July 2019, URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_response_us_cloudact_coverletter.pdf

[145] Council Decision authorising the opening of negotiations, 6 June 2019, URL: https://data.consilium.europa.eu/doc/document/ST-10128-2019-INIT/en/pdf and; https://data.consilium.europa.eu/doc/document/ST-10128-2019-ADD-1/en/pdf.

Microsoft writes about the storage location of the telemetry data: *"Telemetry (service logs, performance logs, errors, and so on) that are key to monitoring and providing a stable service are sent to Microsoft's telemetry data stores."*[146]

From the Company Portal app, diagnostic data are sent to two different endpoints. One of these endpoints is also used for Office telemetry, namely mobile.pipe.aria.microsoft.com. The other endpoint, gate.hockeyapp.net, used to belong to an external party, but that company was taken over by Microsoft.
The transfer of the telemetric personal data from the Company Portal app to Microsoft's servers in the U.S. is based on the EU US Privacy Shield. Microsoft has self-certified under this instrument.[147] Microsoft does not offer the option of processing the diagnostic data about the use of the Company Portal app in the EU.

Although the Privacy Shield, like the SCC, is a legally valid transfer tool approved by the European Commission, there are serious doubts about the future validity of these tools for transfer to the U.S. Both instruments are the subject of proceedings before the European Court of Justice. The Court is asked to decide whether these contracts provide sufficient protection against the risks of mass surveillance in the United States. These risks were revealed by whistle-blower Edward Snowden, also with regard to the interception of data in transmission (transit traffic).[148]

7.3 Azure AD

As mentioned in Section 2.4 (*Azure AD log files*), Microsoft writes that the Azure AD log files are initially stored in the data centre where the Azure AD service is running, i.e. in the case of Dutch government organisations in data centres in the Netherlands and Ireland. "*Log files are (..) originally created and stored in Azure storage in the data centre where the Azure AD service is running*". But subsequently, these log files are scrubbed and stored in Microsoft's long-term database in the U.S.[149]

Microsoft also writes that the data processed with multi factor authentication are always processed exclusively in two data centres in the U.S., in Iowa and in California.[150] Microsoft writes: "*All two-factor authentication using phone calls or SMS originate from U.S. datacenters and are also routed by global providers.*"[151] This also applies to digital push messages. Microsoft writes: "*Push notifications using the Microsoft Authenticator app originate from U.S. datacenters. In addition,*

[146] Microsoft, Data storage and processing in Intune, 18 May 2018, URL: https://docs.microsoft.com/en-gb/intune/protect/privacy-data-store-process
[147] Microsoft is an active participant to the Privacy Shield: https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK&status=Active.
[148] In the case C-311/18, the European Court of Justice takes the facts into account which are determined in the case of the Austrian legal expert Max Schrems against the Irish Data Protection commissioner (DPC). The Advocate General has published its advice on 19 December 2019, ECLI:EU:C:2019:1145. The Dutch Ministry of Foreign Affairs publishes an overview of the different steps in this procedure, via: https://ecer.minbuza.nl/ecer/hof-van-justitie/nieuwe-hofzaken-inclusief-verwijzingsuitspraak/2018/c-zaaknummers/c-311-18-facebook-ireland.html. The other case is case T-738/16. This case is submitted by the French NGO La Quadrature du Net, on 9 December 2016. The hearing in this case would take place on 1 and 2 July 2019, but is deferred until the court has ruled in the (above mentioned) Schrems 2-case.
[149] URL: https://aka.ms/aaddatawhitepaper
[150] Microsoft, Identity data storage for European customers in Azure Active Directory, 4 March 2019, URL: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-data-storage-eu
[151] Idem.

device vendor specific services may also come into play and these services maybe outside Europe."[152]

In general, the use of the MS Authenticator app is recommended to enforce compliance with an organisation's information security policy. Alternatively, employees can use other authentication providers, such as Google, if not prohibited by the government organisations.

Because some of the data processing exclusively takes place in the USA, government organisations cannot choose to have personal data processed exclusively in the Western European GEO when they deploy Intune.

8. Techniques and methods of the data processing

Section 1 provides a general description of the nature of the data processing via Intune on the four different platforms, in combination with the Company Portal app and the Azure Active Directory. Section 2 describes the personal data that Microsoft and government organisations process via this service. Section 3 describes the privacy choices that administrators and users (employees) can make and explains the differences between pseudonymisation and anonymisation. This Section 8 discusses two special processing techniques: (1) the way in which Microsoft collects data via the Company Portal app and similar functionality in Windows 10 Enterprise and (2) the ways in which Microsoft can combine data of a user over time.

8.1 Telemetry data collection via the Company Portal app and Windows 10 Enterprise

Microsoft built separate software into the Company Portal app that collects data about the device and stores these snapshots on the device. The telemetry client in the Company Portal app regularly sends these snapshots, in batches, to Microsoft's servers in the United States. Similar to the way in which Microsoft collects telemetry data about the use of Windows 10 and Office 365 ProPlus, Microsoft encodes the telemetry data about the use of Office in an unknown binary format.

These are telemetry data. As explained in Section 3.1 (*Privacy Choices Intune and Azure AD*), employees can influence the data collection via the app and the similar functionality in Windows 10 Enterprise on their own device, by turning off data sharing in the app or by setting the telemetry level to "Basic" or "Security". Administrators can help by centrally blocking the sending of usage data from iOS and iPadOS devices, but not (yet) for other devices.

Microsoft did not publish public documentation on how often the Company Portal app captures data or how often the client sends the collected data to the Microsoft servers. Technically, the app's diagnostic data are sent to various endpoints in the U.S., as explained above, in Section 7.2 (*Intune Company Portal app*).

System administrators and users cannot easily see what data are being collected and sent through the app. There is no Data Viewer Tool to view the telemetry data. As explained in Section 2.3 (*Data processed by Microsoft through the Company Portal app*) 9 and 10 telemetry messages sent from the iOS and macOS

[152] https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-data-storage-eu

Company Portal app, were sent respectively. Microsoft did not publish any information about the content of these messages, which may contain several fields. It was not possible to decode the telemetry flow from Android. Since March 2020, the telemetry stream from macOS is similarly protected against interception with certificate pinning.

8.2 Big data processing

Microsoft publishes much detailed information about the types of personal data it collects through the Intune MDM and MAM cloud services. In contrast, Microsoft did not publish any information about the rules governing the collection of information by the Company Portal app. As explained in Section 7 (*Transfer of personal data outside of the EU*), it is likely that Microsoft stores the diagnostic data from its Azure cloud services together with diagnostic data from Office 365 and Windows 10 in one central long-term database, called Cosmos.

A former Microsoft engineer gave a presentation on the architecture of Cosmos. He explained that Cosmos not only contains these diagnostic data, but also data from Skype, Xbox, Bing, Ads and more.[153] The engineer explains: "*Teams put their data in Cosmos because that is where the data they want to join against is.*" He also indicates that by 2015 there was a cluster of more than 50,000 servers.[154]

In an earlier presentation on Cosmos in 2011, two former Microsoft engineers explained:

"*We ingest or generate a couple of PiB every day*

- *Bing, MSN, Hotmail, Client telemetry*
- *Web crawl snapshots*
- *Structured data feeds*
- *Long tail of other data sets of interest*"[155]

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

9. Legal and policy framework: e-Privacy Regulation

This section only describes the additional obligations arising from the future E-Privacy Regulation. In view of the limited scope of this DPIA, other statutory obligations or frameworks (for example in the field of information security, such as BIO) have not been elaborated on in this report.

The Dutch DPA's research report on Windows 10 telemetry data[156] states that certain rules from the current e-Privacy Directive apply to the placement of information on devices via a built-in telemetry client that is delivered via the Internet. The same rule applies to the recording of information about the use of

[153] Presentation Eric Boutin. Meetup 5 November 2015, URL: https://www.slideshare.net/MemSQL/how-microsoft-built-and-scaled-cosmos (URL last visited and documented 12 July 2019)
[154] Idem, slides 8 en 13.
[155] Pat Helland and Ed Harris, Cosmos, Big Data and Big Challenges, 26 October 2011, URL: http://web.stanford.edu/class/ee380/Abstracts/111026a-Helland-COSMOS.pdf (URL last visited and documented 12 July 2019)
[156] Dutch DPA, report definitive findings Microsoft Windows 10, Attachment 1, p. 26.

Intune via the Company Portal app, and the transmission of this information via the Internet.

The consequences of this provision are far-reaching, as it requires clear and complete information to be provided to the user prior to data processing. In addition, the processing must in principle be based on the user's consent, unless a specific legal exception applies. Part B of this DPIA discusses the (im)possibility of obtaining employee consent for the processing of diagnostic data on the use of the Company Portal app.

The current ePrivacy Directive (as implemented in the Netherlands in Chapter 11 of the Telecommunications Act) also includes rules on the confidentiality and destruction of data from the content and on communication behaviour. Article 5(1) obliges the Member States to guarantee the confidentiality of communications and related data traffic, via public communications networks and public electronic communications services. Article 6(1) obliges providers of public telecommunications services to remove or anonymise the data traffic as soon as they are no longer necessary for the transmission of the communication. Although this ePrivacy Directive does not apply to providers of software in the cloud (which always involves communication via a public electronic communications network), the future ePrivacy Regulation will make these rules applicable to Microsoft as a provider of e-mail and voice services.[157]

On 10 January 2017, the European Commission published a proposal for a new ePrivacy Regulation.[158] The proposed Article 8(1), *Protection of information stored in and related to end-users' terminal equipment*, extends the current consent requirement for cookies and similar techniques to the use of all processing and storage capabilities of terminal equipment.
The European Parliament adopted its position on 23 October 2017. It added a specific exception for updates and in relation to employees. The EP proposes to add two new exceptions to the consent requirement in Article 8(1), namely when it is necessary for security updates and for the performance of work by employees.

> *it is necessary to ensure security, confidentiality, integrity, availability and authenticity of the terminal equipment of the end-user, by means of updates, for the duration necessary for that purpose, provided that:*
> *(i) this does not in any way change the functionality of the hardware or software or the privacy settings chosen by the user;*
> *(ii) the user is informed in advance each time an update is being installed; and*
> *(iii) the user has the possibility to postpone or turn off the automatic installation of these updates;*

The EP also suggested:

> *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;*

[157] See consideration 22 in the ePrivacy directive 2002/58/EG, revised in 2009 by the Citizens' Rights Directive 2009/136/EG: "*The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed*."
[158] European Commission, Proposal for a Regulation on Privacy and Electronic Communications, 10.1.2017 COM(2017) 10 final, URL: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

(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 ePrivacy Regulation for two and a half years, since October 2017. The most recent complete text dates from 6 March 2020.[159]

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

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

(Art 8 (1) The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:
(…)
(c) it is necessary for providing a service requested by the end-user;
~~(da): it is necessary to maintain or restore the security of information society services, prevent fraud or detect technical faults for the duration necessary for that purpose;~~
~~or~~
~~(e) it is necessary for a software update provided that:~~
~~(i) such update is necessary for security reasons and does not in any way change the privacy settings chosen by the end-user,~~
~~(ii) the end-user is informed in advance each time an update is being installed, and~~
~~(iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates; or~~
(g) it is necessary for the purpose of the legitimate interests pursued by a service
provider to use processing and storage capabilities of terminal equipment or to collect
information from an end-user's terminal equipment, except when such interest is
overridden by the interests or fundamental rights and freedoms of the end-user. The end-user's interests shall be deemed to override the interests of the service provider where the end-user is a child or where the service provider processes, stores
or collects the information to determine the nature and characteristics of the end-user
or to build an individual profile of the end-user or the processing, storage or

[159] Council of the European Union, Interinstitutional file 2017/0003 (COD), Brussel 6 March 2020, 13080/19 URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6543_2020_INIT&from=EN.For an overview of earlier proposed versions of the regulation by the Council, see URL: https://eur-lex.europa.eu/procedure/NL/2017_3#2019-10-17_DIS_byCONSIL .

collection of the information by the service provider contains special categories of
personal data as referred to in Article 9(1) of Regulation (EU) 2016/679.[160]

The Council explains in the new recital 21b:

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

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

Article 6
1. Providers of electronic communications networks and services shall be permitted to process electronic communications data only if:
(…)
(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors and/or security risks and/or attacks in the transmission of electronic communications, ~~for the duration necessary for that purpose;~~
(c) it is necessary to detect or prevent security risks and/or attacks on end-users' terminal equipment, ~~for the duration necessary for that purpose.~~[161]

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

Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal person having subscribed to the electronic

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

communications service may allow a natural person, such as an employee, to make use of the service in accordance with Regulation 2016/679.

With regards to the use of the processing and storage capabilities of terminal equipment, the Council deleted explanations when consent would be required from recital 21:[162]

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

In sum, it appears that the ePrivacy Regulation continues to contain a consent requirement for the collection of information from devices from users where this is not necessary to provide a service. In its last version the Council proposes to introduce the legitimate interest ground. This is diametrically opposed to the position of European Parliament and Commission. It therefore seems likely that the current ePrivacy Directive, which does not contain such a balancing of interests possibility, will continue to apply in the next few years.[163]

[162] Idem.
[163] It is not clear when the new ePrivacy Regulation (2017/0003/COD) will enter into force. Progress can be tracked via: https://eur-lex.europa.eu/procedure/EN/2017_3 The Ministers of the Member States have not yet reached agreement in the Council (in March 2020) on their negotiating position on the ePrivacy Regulation. Thereafter, the trialogue should start negotiations with the (new) European Commission and the (new) European Parliament. Subsequently, a transitional period of 1 or 2 years will apply. In any case, the scope of the scope of the Telecommunications Directives and the ePrivacy rules will be extended via the Electronic Communications Code (2016/0288(COD), final vote by the European Parliament on 14 November 2018) after a transitional period of 2 years, at the end of 2020, from the current handful of providers of telephony and Internet services to all web-based equivalent providers.

10. Retention periods

In the Data Protection Addendum that is part of Microsofts Online Services Terms, there is one section on retention periods. This shows that Microsoft stores the Customer Data of core online services such as Intune for 90 days after termination of the subscription. Microsoft actually deletes the Customer Data and personal data after another 90 days.

> *Data Retention and Deletion*
> *At all times during the term of Customer's subscription, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service.*
>
> *Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data within an additional 90 days, unless Microsoft is permitted or required by applicable law to retain such data or authorized in this contract.*
>
> *The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data or Personal Data as described in this section.*[164]

Microsoft writes that it does not destroy the content of Intune records, but marks them as deleted (soft delete). The data about users will be saved as long as government organisations have a subscription to Intune, plus another six months after that. If the administrators want to see only the current data, they have to apply a filter, *IsDeleted = FALSE*.

Dimension tables in the entity lifetime

In order to store the history of state changes in entities, Intune doesn't delete records. Instead it marks the record as deleted. This is called a soft-delete. The dimension tables use various metadata columns to track the lifetime of records.

10.1 Intune MDM and MAM log files retention periods

Microsoft writes about Intune's retention periods: *"In general, personal data is retained by Intune until 30 days after the user is removed from Intune management.*
Telemetry data collected as part of Intune usage is retained for a maximum of 30 days. Audit logs are retained for up to one year." [165]

Microsoft allows administrators to export the various Intune log files, and save them for a period of time of their choosing. This includes Audit logs, Operational logs and Organizational logs for device compatibility.

Microsoft writes: "*For security purposes Intune may maintain audit logs for user and device actions for a period of one year. These logs are automatically deleted after the one-year retention period. (…) Admins can't delete audit logs. These audit events are retained for one year.*" [166]

---

[164] Microsoft Online Services DPA, January 2020.
[165] Microsoft, Data storage and processing, 18 May 2018, URL: https://docs.microsoft.com/en-gb/intune/protect/privacy-data-store-process
[166] Microsoft, Audit, export or delete personal data in Intune, 18 May 2018, URL: https://docs.microsoft.com/en-gb/intune/protect/privacy-data-audit-export-delete

Microsoft describes the possibility, by using the Intune Data Warehouse, that Intune takes a snapshot of the status every day at midnight, and stores this snapshot in the data warehouse. "*The duration of held snapshots vary from fact table to fact table. Some may hold seven days, others 30 days, and some even longer durations*."[167] Government organisations have to decide for themselves, in an individual DPIA, how long they need to retain these data, whether they want to use this Intune Data Warehouse, or export the data to combine them with logs from other security information and event management tools (SIEM logs).

If a government organisation does not use the export options, it only sees the latest known state of affairs in the audit logs. The maximum retention period is 30 days. This period can occur if a device was not connected to the Internet for 29 days, for example. Nonetheless, the administrators cannot choose a shorter retention period than 1 year for the audit logs currently.

10.2 Retention period Azure AD audit and sign-in logs

Microsoft explains that the retention period of the Azure AD Audit log files varies between 7 and 30 days for activity reports, and between 7 days and 90 days depending on the type of customer subscription (Premium P1 30 days, Premium P2 90 days).[168] Activity reports are large files. This makes it unattractive for organisations to keep the data for more than 30 days.

10.3 Retention period log files in Cosmos database

Microsoft does not describe in its contract and public documentation the retention periods that the company itself determines in central database systems such as Cosmos. The umbrella DPIA's for SLM Rijk over Office 365 ProPlus, Office Online and the mobile Office apps show that Microsoft stores most of the telemetry data from Office 365 for 30 days, but also stores certain data in Cosmos for a long time, up to 18 months.

As explained in Section 4.3 (*Purposes Azure AD*), Microsoft published a (public) audit report on Azure (testing against ISO 27001 and 27018).[169] In this report, the auditor notes that Microsoft is creating at least one log file for its own (security) purposes. He writes that these data are stored for 30 to 90 days in the Geneva monitoring tool, and stored in the Cosmos database for one year or as much longer as necessary (*as needed*).[170]

As explained in Section 8.2 (*Big data processing*), it is likely that Microsoft will store certain log files about the Azure AD, and the Company Portal app in the central Cosmos database. Microsoft removes the directly identifiable data from the diagnostic data, and stores the identifiers in a *hashed* format, as described in Section 3.2 (*Anonymisation and pseudonymisation*). This instead of storing the original data. Based on the NIST checks with regard to log files referred to in this section, it is plausible that the service teams can also undo this form of pseudonymisation with regard to log files other than Office 365 with the aid of the continuous data collection.

---

[167] Microsoft, Microsoft Intune Data Warehouse data model, 12 April 2019, URL: https://docs.microsoft.com/en-us/intune/developer/reports-ref-data-model
[168] Microsoft, How long does Azure AD store reporting data? 13 November 2018, URL: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention
[169] BSI Assessment report on compliance standard ISO/IEC 27001:2013 and ISO IEC 27018:2014 by Microsoft Azure, published on 23 August 2018, p. 13.
[170] Idem.

Part B. Assessment of the lawfulness of data processing

In the second part of the DPIA the lawfulness of data processing will be assessed. This part describes the grounds and gives 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

All processing operations must have a ground in Article 6(1) of the GDPR. Essentially, for processing to be lawful, this article demands that the data controller bases the processing on the consent of the user, or on a legally defined necessity to process the personal data.

The appropriate legal ground depends on Microsoft's role as (joint) controller, or as processor. Thanks to the improved privacy conditions that SLM Rijk negotiated with Microsoft, Microsoft behaves as a data processor for the processing of personal data via Intune MDM, MAM and the Azure AD. As a result, government organisations must have a legal ground for the processing of these personal data as (independent) controllers.

However, the privacy improvements do not (yet) apply to data processing via the Intune Company Portal app, and comparable functionality from Windows 10 Enterprise. Government organisations are joint controllers with Microsoft for the data processing via the app. This has consequences for the possible legal grounds.

11.1 Intune MDM, MAM and the Azure AD

Microsoft qualifies itself via the OST as a processor for Intune MDM, for Intune MAM and for the Azure AD. As explained in Section 5.2 of this report (*Microsoft as processor for Intune MDM and MAM and Azure AD*), only a data controller may determine the purposes of the processing. Under the improved privacy terms, Microsoft may only process the data from and about the cloud services for three purposes, and only to the extent that processing for those purposes is proportionate. These three purposes are: (1) the technical provision and improvement of the service, (2) keeping the service up to date and (3) keeping the service secure.

As independent data controllers for the processing of personal data via these cloud services, government organisations can successfully invoke two of the six possible legal grounds for these three purposes. This concerns the necessity for the performance of the (employment) contract with the employees (Article 6(1)(b) of the GDPR), when it comes to registering and encrypting self-managed (and organisation-administered) devices and processing personal data in order to control access to personal data (authorisation via the Azure AD). If Microsoft were a data controller, it could not rely on the ground of the performance of a contract, because Microsoft does not have a contract with the employees.

The other two grounds on which government organisations can rely, are (i) the performance of a task carried out in the public interest (Article 6(1) e of the GDPR) and (ii) necessity for the purposes of their legitimate interests (Article 6(1)(f) of the GDPR). Of course, the last sentence of Article 6(1) of the GDPR excludes the application of the legitimate interest ground for processing carried out by public authorities in the performance of their tasks. However, the protection of the

personal data on employee devices is secondary to the performance of public tasks by public authorities, and can therefore also be considered as a task primarily exercised under private law. As explained in Recital 47 of the GDPR, the legal ground of necessity for the legitimate interest (Article 6(1) f) is more likely to exist where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. On the other hand, Intune is also used to protect the communications with other data subjects on employee devices. Therefore, government organisations can also invoke the legal ground of the performance of their public tasks.

Both legal grounds require an assessment of the necessity of the personal data processing, of the proportionality and availability of alternative, less infringing means to achieve the same legitimate purposes (subsidiarity). In the arguments below, both legal grounds are discussed simultaneously.

It is necessary to be able to delete personal data on the devices and in Microsoft apps, in order to protect the interests of all data subjects about whom data are processed via the self-managed devices. Encryption and the possibility of deleting personal data also serves the legitimate interest of government organisations themselves and is necessary for the performance of a task carried out in the public interest because the security and data breach requirements of the GDPR oblige government organisations to take adequate security measures. This legitimate interest and necessity also applies to the keeping of log files and monitoring of compliance, not only by the employees, but especially by the system administrators with access to the log files and settings.

A successful appeal to the legal ground of consent is precluded because the employees have no choice as regards the processing of personal data concerning them by Microsoft and by the government organisations themselves. As employees and as system administrators, they cannot freely refuse to give their consent in view of the dependence on their employer. The Data Protection Authorities, united in the European Data Protection Board, write: *"Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent."*[171]

Table 4: Purposes, role and applicable legal grounds for Intune

Purpose	Ground	Organisations as controller
(Technical) delivery and improvement of the service including debugging	Consent	X No free choice for employees
	Contract	√ Authorisation and registration of the self-managed equipment in Intune
	Legal obligation	X No law requiring the use of Intune
	Legitimate interest/public interest	√ Limited logging data employees via Intune and system administrators for data breach compliance and GDPR security obligations

[171] Article 29 Working Party, WP 259 version 01, Guidelines on Consent under Regulation 2016/679. Adopted on 28 November 2017. At last Revised and Adopted 10 April 2018, p. 7-8. URL: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030 Also see consideration 43 of the GDPR.

Keeping the service up to date	Consent	X No free choice for employees
	Contract	√ Necessary measure Microsoft to prevent unauthorised access
	Legal obligation	X No law requiring the use of Intune
	Legitimate interest/public interest	√ Necessary measure Microsoft to prevent unauthorised access
Securing the service (platform security)	Consent	X No free choice for employees
	Contract	√ Necessary measure Microsoft to prevent unauthorised access
	Legal obligation	X No law requiring the use of Intune
	Legitimate interest/public interest	√ Necessary measure Microsoft to prevent unauthorised access

11.2 Intune Company Portal app

As explained in Section 5.3 of this report (*Microsoft as controller for the Company Portal app*), Microsoft considers itself to be the (independent) controller for the data processing via the Intune Company Portal app, comparable built-in functionality in Windows 10 Enterprise, and the debug log. However, in practice, government organisations are joint controllers for this data processing with Microsoft because that the use of the Company Portal app is mandatory, and similarly data of employees working on a laptop with Windows 10 Enterprise are processed once an organisation deploys Intune.

Microsoft does not request consent from employees when installing the Company Portal app to send telemetry to itself or to the employer in case of a debug log. However, this consent is required by law, at least for part of the data Microsoft collects from the device, under Section 11.7a of the Telecommunications Act. This is because not all data comply with the exception clause that they are strictly necessary to provide the information society service requested by the subscriber or user. For example, the names of all Microsoft apps installed on a Windows 10 Enterprise laptop, or the e-mail address, the e-mail alias or the self-chosen name of the device are not necessary to provide the service. Providing a (well hidden) opt-out after the app has been installed, does not amount to obtaining consent. Even though users actively choose to send a debug log to Microsoft, since they are not informed about the contents of the log file, and can not read nor analyse the contents, this action cannot result in obtaining legally valid, informed consent either.

As a controller, Microsoft allows itself to process personal data from telemetry and debugging files for seventeen purposes, as described in its general privacy statement. However, as a joint controller with Microsoft, government organisations can only rely on the basis of necessity for the performance of the (employment) contract when they require an employee to install the app, or necessity for its legitimate or public interest for three purposes.

These three purposes are:

1. (Technical) delivery and improvement of the app including troubleshooting and bug fixing
2. Keeping the app up to date (including resolving issues caused by the updates)
3. Securing the app

For the remaining 14 purposes for which Microsoft wants to process the data as the controller, neither government organisations nor Microsoft have any legal basis. These purposes are therefore not dealt with separately in table 5 below.

Table 5: Purposes, role and applicable ground for the Company Portal app

Purpose	Ground	Microsoft as controller	Organisations as controllers
(Technical) delivery and improvement of the app including debugging	Consent	X	X No free choice for employees
	Contract	X No contract with employees	√ registration via the self-managed devices in Intune
	Legal obligation	X No law requiring the use of Intune	X No law requiring the use of Intune
	Legitimate interest/public interest	X No personal data processing without instruction from customers/Microsoft cannot claim tasks in the public interest	√ Limited log data on the operation of the app, necessary for data breach and security obligations GDPR
Keeping the app up to date	Consent	X	X No free choice for employees
	Contract	X No contract with employees	√ Necessary measure Microsoft to prevent unauthorised access
	Legal obligation	X No law requiring the use of Intune	X No law requiring the use of Intune
	Legitimate interest/public interest	X No personal data processing without instruction from customers/ Public interest	√ Necessary measure Microsoft to prevent unauthorised access
Securing the app	Consent	X	X No free choice employees
	Contract	X No contract with employees	√ Necessary measure Microsoft to prevent unauthorised access
	Legal obligation	X No law requiring the use of Intune	X No law requiring the use of Intune

	Legitimate interest	X No personal data processing without instruction from customers/ Public interest	√ Necessary measure Microsoft to prevent unauthorised access
The remaining 14 purposes for which MS can process the data as a controller	Consent	X	X
	Contract	X	X
	Legal obligation	X	X
	Legitimate interest/Public interest	X	X

12. Special categories of data

Special categories data are defined in Article 9 of the GDPR: "*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 shall be prohibited.*"

Government organisations **do not process any special categories of personal data** via Intune or the Azure AD, nor do they process any criminal data as referred to in Article 10 of the GDPR. They can, however, destroy sensitive data if they delete all data from a device via Intune MDM.

In its guidelines on the use of cloud computing services, the Data Protection Supervisor of the European institutions, the EDPS, explains that the concept of special categories of personal data should be interpreted in a very broad way when assessing the risks for data subjects. The EDPS writes: *"Nevertheless, this is not the only factor determining the level of risk. Personal data that do not fall under the mentioned categories might lead to high levels of risk for the rights and freedoms of natural persons under certain circumstances, in particular when the processing operation includes the scoring or evaluation of individuals with an impact on their life such as in a work or financial context, automated decision making with legal effect, or systematic monitoring, e.g. through CCTV."* [172] The EDPS also refers to the criteria of the (former) Article 29 Working Party of data protection supervisors in the EU when the performance of a DPIA is mandatory.[173]

The keeping and inspection of log files on the behaviour of system operators may involve personal data of a sensitive nature. The processing of such data can involve similarly high risks for these employees (the system administrators) as would the processing of special categories of data or criminal data, when the log files are kept and accessed for the purpose of preventing and detecting breaches of policy rules.

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

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

Intune allows administrators to convert the status of self-managed devices from personal to corporate devices. 7 days after such a status change the administrator can see all installed apps on an employee's device, and the full phone number on iOS devices. It follows from the technical research that these overviews of installed apps may also include private apps, such as health apps.

Collecting data from all installed apps on iOS can reveal sensitive data about an employee, for example, if apps are installed that process health data, indicate political opinions, religious beliefs, or sexual orientation. In addition to the tested app with a pregnancy diary, the overview can also include apps about a diet, an app from a political party or movement, an Islamic prayer time app or an app aimed at sexual contacts between men. The risks of this processing for data subjects are considerable, especially now that the research shows that the status change is virtually invisible to data subjects (only by means of a report in a separate screen in the app that a user will never have to open again after installation). Collecting an employee's (private) phone number on iOS devices could lead to *stalking*.

The (repeated) technical inspection of this status change option (see Section 3.1, Privacy Choices Intune and Azure AD) shows that it is not possible for administrators to see the location data of employees from self managed iOS devices. An administrator cannot set the status of such a device to Lost, which is the first step required to gain access to the location data. The only way to use this feature from Intune is to set the device to fully managed via auto enrolment.

In its guidelines on the use of cloud computing services, the Data Protection Supervisor of the European institutions, the EDPS, explains that the concept of sensitive data should be interpreted in a very broad way when assessing the risks for data subjects. The EDPS writes: *"Nevertheless, this is not the only factor determining the level of risk. Personal data that do not fall under the mentioned categories might lead to high levels of risk for the rights and freedoms of natural persons under certain circumstances, in particular when the processing operation includes the scoring or evaluation of individuals with an impact on their life such as in a work or financial context, automated decision making with legal effect, or systematic monitoring, e.g. through CCTV*."[174] The EDPS also refers to the criteria of the (former) Article 29 Working Party of data protection supervisors in the EU when the performance of a DPIA is mandatory.[175]

13. Purpose limitation

Purpose limitation is one of the core principles of Article 5 of the GDPR. Data may only be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*" (Article 5 (1) (b) GDPR). Essentially, this means that the controller must have a specified purpose for which he collects personal data, and can only process these data for purposes

[174] EDPS, Guidelines on the use of cloud computing services by the European institutions and bodies, 10 March 2018, URL: https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf.
[175] Article 29 Working Party, WP 248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, URL: http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236 .

compatible with that original purpose. Controllers must be able to prove compliance with this principle on the basis of Article 5(2) of the GDPR (accountability).

As explained in Section 4.1 of this report (*Limitation to three purposes for cloud services*), Microsoft agreed through the improved privacy conditions that it may in principle only process personal data as data processor for its Online Services, and only for three legitimate purposes, and only if it is proportionate. These purposes are: (1) providing and improving the service technically, (2) keeping the service up to date, and (3) keeping the service secure.

Under the Dutch government privacy amendment, this strict purpose limitation applies to all types of personal data, including diagnostic data, telemetry messages from installed software and apps, and the system-generated event logs on Microsoft's own servers, in addition to the content of customer data.

However, it is not clear whether SLM Rijk will gain access to the log files Microsoft keeps for its own purposes on the Azure AD, as mentioned in Section 4.3 of this report (*Purposes Azure AD*). It is equally unclear if Microsoft stopped processing the Azure AD log files for purposes such as systemic health analysis, system-wide analysis with machine learning and discovering opportunities for product improvement. To verify Microsoft’s compliance with the agreed purposes, SLM Rijk should use its newly acquired right of audit to check that Microsoft no longer processes the data for its own purposes.

Unfortunately, Microsoft does not apply the purpose limitation guarantees to the telemetry data that Microsoft collects and processes via the Intune Company Portal app and the Intune functionality of Windows 10 Enterprise. Purpose limitation is the most difficult principle to observe when processing *big data*, because it is precisely the challenge to gain new insights by linking data in a different way. Section 8.2 of this report (*Big data processing*) describes how Microsoft combines different data flows in the long-term Cosmos database. The data processing is dynamic. Microsoft can add new telemetry messages to the app on the fly, even without first sending a software update. Section 4.2 (*Purposes Company Portal app*) describes that, according to its privacy statement, Microsoft wants to be able to combine data from various services as a controller, and to use data for unspecified types of product innovation, product development, targeted advertising and research.

Because Microsoft does not publish audit reports on processing for which it considers itself data controller, such as the Company Portal app and the Windows 10 operating system, government organisations are not able to see whether the diagnostic messages are being collected lawfully, in accordance with the agreed purpose limitation. Nor is it known whether Microsoft (now) established internal policies regarding the need to collect specific telemetry messages and how and whether those policies are complied with internally. Microsoft does not publish information about the types of personal data and the purposes for which it processes the telemetry data from the Intune Company Portal app, and data subjects cannot monitor the data flow because there is no Data Viewer Tool available to decrypt the data flow.

In sum, the improved privacy conditions of SLM Rijk ensure compliance with the purpose limitation principle with respect to Intune's cloud services. SLM Rijk must check whether Microsoft actually complies with this purpose limitation principle. With regard to the Company Portal app, Microsoft does **not give any guarantees**

regarding compliance with the purpose limitation principle. The seventeen purposes for which Microsoft allows itself to process the telemetry data, including the e-mail addresses of the users, are not sufficiently precise and explicit to allow verification that a specific telemetry message is being collected for a legitimate purpose.

14. Necessity and proportionality

14.1 The principle of proportionality

The concept of necessity is made up of two related concepts, namely proportionality and subsidiarity. The personal data which are processed must be necessary for the purpose pursued by the processing activity. It has to be assessed whether the same purpose can reasonably be achieved with other, less invasive means. If so, these alternatives have to be used.

Second, proportionality demands a balancing act between the interests of the data subject and the data controller. Proportionate data processing means that the amount of data processed is not excessive in relation to the purpose of the processing. If the purpose can be achieved by processing fewer personal data, then the amount of personal data processed should be decreased to what is necessary.

Therefore, essentially, the data controller may process personal data insofar as is necessary to achieve the purpose but may not process personal data he or she may do without. The application of the principle of proportionality is thus closely related to the principles of data protection from Article 5 GDPR.

14.1 Proportionality assessment

The key questions are: are the interests properly balanced? And: does the processing go no further than 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.[176]

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 provides a lot of information about the data it collects and processes through the Intune MDM and MAM cloud log files. Administrators can compare the information that Microsoft publishes with the content of the log files that they can access themselves. This access shows that Microsoft's basic information is in

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

complete. As explained in Section 2.2.1 (*Microsoft Intune MDM*), Microsoft does not mention that it collects the userID, e-mail address, e-mail alias and lastSyncDateTime on all platforms via the app. Moreover, Microsoft does not explain that (and why) it collects the names of a large part of the (pre-)installed Microsoft apps from Windows 10 Enterprise. Because of the lack of explanation this data collection does not meet the requirement of *data minimisation*.

The processing of personal data via Intune MDM constitutes a disproportionate infringement of the privacy rights of data subjects in one respect. Microsoft built an option into Intune MDM to change the management status of a device (see Section 3.1, *Privacy Choices Intune and Azure AD*). The fact that the user of the device, in this case an employee of a government organisation, does not see a warning on the screen of this status change, and that government organisations cannot build in such a warning with a group policy or other central setting, means that administrators can secretly see more information about the self-managed devices than employees think. This concerns only a part of the devices, namely only those devices that are registered by users themselves and therefore have a 'personal' status. The tests executed in September/October 2019 and March 2020 show that when administrators change the status of such personal devices, they can see the names of all installed apps, including all kinds of apps installed for private use. On iOS devices they can see the (complete) phone number. The fact that employees are not warned about this makes the data processing inherently unfair.

Microsoft also provides information about the log files that it makes available to administrators about the Azure AD, but fails to actively inform its Enterprise customers that it also processes log files for its own purposes, and stores 'scrubbed' data from them in Cosmos for a long time (one year or as much longer as necessary). As explained in Section 2.4 (*Azure AD log files*), this is only apparent from a Microsoft white paper that is not actively disclosed. As a result, the system administrators are unable to provide adequate information to data subjects. Because it is not clear which data Microsoft collects for its own purposes, it cannot be assessed whether Microsoft complies with all legal conditions for data processing.

Microsoft does not provide any information at all about the contents of the debug logs and telemetry data from the Company Portal app. Data subjects cannot control the telemetry data flow themselves, because the data are stored and transmitted in encrypted form and Microsoft does not provide a Data Viewer tool. It is also not possible for data subjects to ask their administrator to submit a request for access via the Microsoft DSR tool or to search for personal data in the audit log files, because these files do not contain any information about the telemetry data from the Company Portal app.

The data inspection shows that Microsoft collects a limited number of unique identifiers via telemetry and debug logs. These logs do not contain sensitive information about the behaviour of employees or the content of communications. The actual data collection therefore does not seem disproportionate to the legitimate purpose that government organisations are pursuing with the use of Intune as a means to secure the self-managed devices and to control access to (personal and/or confidential) data.

In sum, the proportionality of these three processing operations cannot be sufficiently assessed due to the lack of transparency. The processing is unfair to data subjects if the administrators can secretly collect more information than the

information that data subjects rely on. However, government organisations themselves can take measures against this by providing employees with better information than Microsoft does at present, and by strictly supervising the activities of the system administrators.

The principles of data minimisation and privacy by design require that the processing of personal data be limited to what is necessary: the data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (Article 5(1)(c) of the GDPR). This means that the controller may not collect and store data that are not directly related to a legitimate purpose. According to this principle, the default settings for the collection of data must be set in such a way that the collection of data is kept to a minimum, by using the most privacy-friendly settings. The technical examination of the various log files shows that Microsoft does not allow administrators to centrally disable the sending of the telemetry logs and the collection of the debug logs (only for iOS and iPadOS). The fact that users can exercise a choice to end the collection and transmission of the telemetry logs shows that their collection is not strictly necessary for the functioning of the Intune service. The fact that Microsoft enabled this data collection by default seems to be 'convenient' rather than necessary, and therefore does not meet the requirement of Article 5(1)(c) of the GDPR that the personal data are limited to what is *necessary for the purposes for which they are processed*.

The principle of storage limitation requires that personal data be kept only as long as necessary for the purpose in question. Data may not be "kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed" (Article 5(1)(e), first sentence, GDPR). This principle therefore requires that personal data be deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller. The text of this provision further clarifies that "*personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject* (Article 5(1)(e), second sentence, GDPR).

As explained in Section 10 (*Retention periods)*, by default the government organisations' system administrators have access to the MDM and MAM log files for up to 30 days. Microsoft explains that it keeps the audit logs for one year, and that administrators cannot influence this period.

Microsoft explains that it stores the Azure AD files for seven to thirty days on behalf of the administrator. At the same time, a public audit report shows that Microsoft keeps certain log files about the use of the Azure AD in Cosmos for one year, or as much longer as necessary.

It is not clear whether Microsoft also stores scrubbed log files about the use of Intune in Cosmos. No information is known about the retention period of the telemetry data from the Company Portal app, but it is likely that this retention period is equal to the retention period for other telemetry data from Office 365, the mobile Office apps and Windows 10, namely 30 days to 18 months.
It is difficult to argue that such old data are necessary, adequate and relevant for the seventeen different purposes for which Microsoft processes the data as the

controller. Of course, some purposes such as 'Research' are so unspecified that it would be impossible to determine any limitation to the data processing.

Although Microsoft provides a great deal of information about the nature and scope of data processing via Intune, and the content of the various types of Intune and Azure AD log files does not contain data that disproportionately infringe on the privacy rights of data subjects, the processing as a whole does not yet meet the proportionality requirements. This is mainly due to the lack of transparency about the nature of the data processing via the (mandatory) Company Portal app, the lack of a central option for administrators to switch off the transmission of diagnostic data for all devices and the unclear further processing of data in Cosmos. The fact that administrators are able to surreptitiously change the status of a managed device is *unfair* and contrary to the principles of privacy by design and data minimisation.

14.2 Subsidiarity assessment

The key question is whether the same objectives can be achieved with less intrusive means.

Microsoft takes the view that its Enterprise customers themselves choose to use its software and services. According to Microsoft, customers can determine the nature of the data processing themselves via privacy settings in the software. This position presupposes that government organisations are free to choose other software. But in reality, that freedom is limited.

Government organisations should carefully consider what Intune features are needed to achieve their information security objectives. In general, they have a clear necessity to encrypt data on self-managed devices and to remotely wipe the devices if necessary. Intune offers many other management possibilities. Intune includes detailed data loss prevention management capabilities such as the prohibition of copying, pasting and storing documents as well as the possibility to force employees to open hyperlinks only with an Intune secured browser. Government organisations should make their own data protection assessment when deploying Intune, and select the least intrusive settings. Such choices should also be made with regard to the ability to turn off the camera, use of the supervised mode that makes it possible to see location data from iOS devices, the possibility to block access to the App stores, use of the Microsoft Defender antivirus/malware functionality and the choice between managing the entire device, or only selected apps.

From the end user's point of view, MDM is a more intrusive than MAM, because MDM makes it possible to change the status of a device from personal to corporate-managed, and because the administrator can delete the entire device in case of loss.

Intune MAM is a more privacy-friendly way to control access to personal data than Intune MDM, especially when it comes to self-purchased, personal devices that are also used for work. Microsoft also explicitly offers the possibility to use Intune MAM without subscribing to Intune, MAM-WE. In the long run, this can be an attractive way of working for employees with BYOD.

Section 16 of this DPIA describes the (low) data protection risks resulting from the processing of personal data via Intune. Therefore, this DPIA does not necessitate government organisations to look for another supplier of comparable security and management options for employees' terminal equipment.

In contrast with productivity software, there are many other suppliers of mobile device management software. Many of these vendors are American, and, to the best of Privacy Company's knowledge, no public study was published yet n the privacy risks and control options associated with the use of this software. There are (at least) three European suppliers:

- SAP Mobile Secure (Germany)
- Matrix42 (Germany)
- Clyd (France, part of Telelogos)

Some other non-European (mainly American, but also two Indian and one Canadian) solution providers for all four platforms are:

- Amtel Netplus Mobility (Maryland);
- Cisco Meraki (California);
- DeviceMax (Kochar Infotech limited, India);
- Hexnode (San Francisco);
- IBM MaaS360 (New York);
- Kaseya (New York);
- ManageEngine (Zoho Corporation, India);
- MobileIron EMM (California)[177];
- SOTI (Canada);
- Steel talon (Kitewire group, Virginia);
- VMware AirWatch (part of the Dell group in the U.S.)

Use of the software of these non-European companies would at least pose some of the same data protection risks for employees, for example with regard to the transfer of personal data to the United States and to India. Furthermore, government organisations should first conduct a pilot with Intune or alternative software in order to arrive at a proper comparison of the privacy risks for data subjects in relation to the information security benefits.

15. Rights of data subjects

The GDPR grants data subjects a number of privacy rights.

15.1 Right to information

First of all, data subjects have a right to information. This means that controllers should publish easily accessible, comprehensible and concise information, in clear language, on, inter alia, their identity as data controllers, the purposes of the data processing, the intended duration of the storage and the rights of data subjects.

Since February 2019, Microsoft publishes comprehensive information on the diagnostic data that system administrators can see through the various log files on the use of Intune MAM and MDM on the various platforms (see Section 2.2 of this report, *Three types of Intune log files*). Microsoft expects the system administrators, as controllers, to provide the employees with an insight into what data they are collecting.

[177] These suppliers are listed in a recent overview of alternatives for Intune, FinancesOnline, Intune Alternatives, 22 August 2019, URL: https://alternatives.financesonline.com/p/intune/ Another long list of alternatives can be found at: https://www.getapp.com/security-software/a/microsoft-intune/alternatives/ Both lists look at software that is recommended for more than 10,000 people and is suitable for all four platforms (iOS, macOS, Windows and Android). The list in this report is only meant as illustration and does not complain representativity or exhaustiveness.

As described in Section 1.2.2 of this report, Microsoft shows data subjects an overview of the main types of data that it does and does not collect via the Intune Company Portal app. However, Microsoft does not provide any information about the diagnostic personal data that it processes itself through the Company Portal app and the debug log.

Microsoft does not provide information about the existence and content of the telemetry messages in technical language for admins. Neither admins nor data subjects are able to view the data flow in readable form, because Microsoft does not provide a Data Viewer tool, as it does for the telemetry from Office 365, Windows 10, and very recently, for some of the Office apps.

Transparency is also essential to enable data subjects to exercise their rights. Microsoft offers an opt-out option to data subjects for sending telemetry via the app, but due to a lack of transparency, data subjects do not know that telemetry is being sent, and that there is an opt-out option.

The DPIA concludes that Microsoft and government organisations are in fact joint controllers at present for the processing of the telemetry data from the Company Portal app. Government organisations should therefore inform their employees about the nature and scope of the data processing via Intune.

Due to the lack of transparency about data processing via the Company Portal app, government organisations, as joint controllers with Microsoft, are actually unable to adequately inform their employees. On the basis of the results of the technical research performed for this DPIA, they can however provide their employees with better information than Microsoft currently provides. This is explained in Section 17 of this report, with proposals for concrete mitigating measures.

15.2 Right of access

Secondly, data subjects have the right of access to the personal data concerning them. Upon request, data controllers must inform data subjects whether they are processing personal data about them. If this is the case, data subjects should be provided with a copy of the personal data processed, together with information about the purposes of processing, recipients to whom data have been transmitted, the period for which personal data are to be stored, and information on their further rights as data subjects, such as filing a complaint with the Data Protection Authority.

As described in Sections 2.2.1 and 2.2.2, Microsoft's Export IntuneData script offers administrators a good opportunity to search the Intune log files for the latest status of a specific employee's device. Using Microsoft's Data Subject Request tool, administrators can view the Azure AD log files. This does not, however, give data subjects access to the log files that Microsoft processes for its own purposes, and which it stores in Cosmos in a 'scrubbed' form for a long time (one year or as much longer as necessary). As explained in Section 2.4 (*Azure AD log files*), the existence of this processing is only apparent from a Microsoft white paper that is not actively disclosed.

In its Intune information pages, Microsoft has a page dedicated to the exercise of rights by data subjects. Under the heading "Export personal data", Microsoft writes: *"Admins can export end user personal data, including accounts, service data, and associated logs to comply with Data Subject Rights requests. It's up to you and your organization to decide whether or not to provide the data subject*

with a copy of the personal data or if you have a legitimate business reason to withhold it. If you decide to provide it, you can provide them with a copy of the actual document, an appropriately redacted version, or a screenshot of the portions you have deemed appropriate to share.
To export a user's personal data, you can use:

- *the Intune MDM Device blade to export a list of devices. You can also copy device data directly.*
- *the Export-IntuneData.ps1 script."* [178]

Microsoft does not mention any possibility to request access to the telemetry data from the app it collects for its own purposes. In theory, data subjects could make a direct request for access to Microsoft as the (joint) data controller. No separate request for information was sent to Microsoft, also because an earlier request for access to the telemetry data from the mobile Office apps for government organisations remained unanswered.

It is up to government organisations as controllers to adequately inform employees about the possibility of submitting a data subject access request to the telemetry data, and the limited scope thereof. Concrete mitigating measures are proposed in Section 17 of this report.

15.3 Right to rectification and erasure of data

Thirdly, data subjects have the right to have inaccurate or outdated information corrected, incomplete information completed and - under certain circumstances - personal information deleted or the processing of personal data restricted.

Microsoft writes that administrators cannot correct or supplement the information in the Intune interface and logs about devices or apps. "*If an end user wants to correct any personal data (like the device name), they must do so directly on their device. Such changes are synchronized the next time they connect to Intune.*"[179]

Microsoft describes three, mainly theoretical, ways to remove personal data from Intune management:

- Deleting the user from Azure Active Directory
- Resetting the device to the factory settings
- The user removes himself[180]

The first option means that the user must be deleted from the Azure AD. This option is therefore only interesting if the employment contract is (permanently) terminated. The second option is useful for corporate devices: when a device needs to be wiped clean to be handed over to a new employee. The third option, that users remove their personal Android, Apple or Windows device from the Intune administration without the help of the administrator, means that employees are no longer allowed to use the organisation network and associated software facilities, and can therefore no longer (properly) do their work. Even more rigorous is the nuclear option to cancel the tenant's entire Intune account.

Given the retention period of up to one month of the Intune log files, the situation is unlikely to arise that the personal data are no longer needed for the purposes for which they were collected or otherwise processed (Article 17(1)(a) of the

[178] Microsoft, Audit, export, or delete personal data in Intune, 18 May 2018, URL: https://docs.microsoft.com/en-gb/intune/protect/privacy-data-audit-export-delete
[179] Microsoft, Audit, export, or delete personal data in Intune, 18 May 2018, URL: https://docs.microsoft.com/en-gb/intune/protect/privacy-data-view-correct
[180] Microsoft, Audit, export, or delete personal data in Intune, 18 May 2018, URL:

GDPR). Nor is it likely that during this short period government organisations or Microsoft would not have any overriding legitimate interests in the limited processing of personal data (Article 17(1)(c) of the GDPR).

However, it is problematic that Microsoft does not offer the possibility to request correction or deletion of the telemetry data from the app, which it collects for its own purposes. These data may be stored for one year or longer, when the data are stored in Cosmos in pseudonymised form.

It is up to government organisations as controllers to adequately inform employees about the (im)possibilities of correction and removal. Concrete mitigating measures are proposed in Section 17 of this report.

15.4 Right to object to profiling

Fourthly, data subjects have the right to object to an exclusively automated decision if it has legal effects. When processing data about the use of Intune, the Azure AD and the Company Portal app, there are no known decisions made by Microsoft that have legal consequences or other significant consequences for the rights and freedoms of data subject. Therefore, this specific right of objection does not apply here.

15.5 Right to data portability

Employees have a right to data portability if their personal data are processed on the basis of the necessity of the execution of the (employment) contract. As explained in points 11.1 and 11.2, government organisations can rely on this ground if the processing is limited to the three specifically mentioned legitimate purposes. Namely: to provide the service (technically) including the detection and resolution of problems, the sending of updates and the provision of a secure service. This is not yet the case for the processing of personal data via the Company Portal app.

If, at the request of an employee, the administrators make use of the export option of the latest available status of the device as described in Section 15.2 (*Right of access*), this export can also be regarded as an interpretation of the right to data portability. The data are made available in JSON format and in the absence of a specific standard for MDM services, this can be regarded as a common machine-readable form.

This is mainly a theoretical compliance. In practice, Intune is set up as a tool for system administrators to check the compliance status of devices, and not as a means for data subjects to keep track of their own compliance status. It is highly questionable whether the data subject (or a third party) can continue the processing himself (or have the data processed by a third party), based on the receipt of such a one-time export.

15.6 Right of complaint

Finally government organisations , as they are joint controllers with Microsoft for data processing via the Intune Company Portal app, must inform employees of their right to file a complaint internally with the two DPOs and externally with the Personal Data Authority. This measure is explained in Section 17 of this report.

In sum, neither Microsoft nor government organisations are currently in a position to (fully) honour data subjects' rights with respect to data processing via the Intune Company Portal app.

Part C. Discussion and Assessment of the Risks for data subjects

16. Risks

This part contains a discussion and assessment of the risks for the rights and freedoms of data subjects resulting from the processing of personal data via Intune. This part starts with an overall identification of the risks in relation to the rights and freedoms of data subjects, resulting from the processing of information about their devices.

Part D of this DPIA provides an analysis of the remaining risks after the mitigating technical, organisational, and legal measures taken by Microsoft as a result of the negotiations with SLM Rijk.

16.1 Identification of the risks

There is no risk that the administrators of government organisations or Microsoft will be able to view the content of data that employees process on their self-managed devices via Intune. Registration of mobile devices in Intune makes it possible to delete all or part of the data on the devices, and to block certain functionalities such as copying or using the camera. Intune does not allow access to photos, files, e-mail or social media accounts, for example.

However, a few different types of risks can occur when processing personal data about the use of mobile devices via Intune MDM and MAM, in combination with the Azure Active Directory and Intune Company Portal app. These risks are explained below.

16.2 Risk assessment

The risks can be classified into the following five main categories:

1. Loss of control over the use of data
2. Loss of confidentiality
3. Impossibility for data subjects to exercise their rights
4. Reidentification of pseudonymised data
5. Unlawful (further) processing

These risks have to be assessed against the likelihood of the occurrence of these risks and the severity of the impact.

The UK data protection commission ICO provides the following guidance:
Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk. [181]

In order to weigh the severity of the impact, and the likelihood of the harm for these generic risks, this report combines a list of specific risks with specific circumstances of the specific investigated data processing.

[181] ICO, How do we do a DPIA?, URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/.

16.2.1 Unauthorised access by system administrators

As explained in Section 14.1 (*Proportionality Assessment*), the processing of personal data via Intune MDM constitutes a disproportionate infringement of the privacy rights of data subjects in one respect. The fact that system administrators can secretly change the management status of a device (see also Section 3.1, *Privacy choices Intune and Azure AD*) can lead to unlawful processing of an employee's sensitive private data. As explained in Section 12 (*Special categories of data*), the collection of an employee's (private) telephone number could lead to *stalking*. Section 3.1 (*Privacy choices Intune and Azure AD*) explains that it is possible to see the full telephone number on iOS devices and all installed apps on macOS, Android and iOS devices. The installed apps may reveal information of a sensitive nature about an employee if, for example, apps are installed that process health data, indicate political opinions, religious beliefs or sexual orientation. Think of dietary or pregnancy diary apps, a political party or movement app, an Islamic prayer time app, or an app that focuses on male sexual contact.

The fact that the data subject, an employee of government organisations, does not receive a prominent warning or consent request in the event of such a change of status, and that government organisations cannot build in such a warning with a group policy or other central configuration option, means that administrators can secretly see more information about the self-managed devices than employees think.

Government organisations already work with role-based access restrictions and should use the differentiated access and authorisation possibilities for administrators in Intune. Additionally, they should develop a policy to actively monitor the actual behaviour of administrators in Intune. In that case, the likelihood is low that the risks will occur of loss of control for data subjects over the use of the data, loss of confidentiality and unlawful (further) processing. If the organisations ensure through these measures that the chance of occurrence of the risk is low, the data protection risks for data subjects are low, despite the potentially high impact on individual data subjects.

16.2.2 Chilling effect personnel monitoring system

With Intune MDM, administrators collect detailed information about employees' self-managed devices and their latest contact moments. Because the administrators also have access to extensive Azure AD activity reports and sign-in log files, they can, in principle, create profiles of the working behaviour of employees much more easily than before. The correlation of data from the Intune and Azure AD log files is much easier than in situations where information on individual employee behaviour is only available in separate SIEM log files.

Knowing that organisations can process detailed data about work patterns can have a *chilling effect* on employees. A chilling effect is the feeling of pressure that can be created in a person by monitoring his or her behavioural data, which can prevent him or her from exercising his or her legitimate rights.[182] The data on the self-managed devices, including the self-chosen name of a device, and the logon and log-off times can provide information about personal preferences and work behaviour.

Using Microsoft Intune can give employees the impression that administrators can see everything they do on their devices, including private activities. That is why it

[182] Merriam-Webster Online Dictionary, "chilling effect", URL: https://www.merriam-webster.com/legal/chilling effect.

is important that government organisations provide clear information about what they can and cannot see, and under which conditions they can use data from the log files. Government organisations could (in theory) use these log files as a basis for a negative assessment of an employee or consult them to identify individual misconduct, for example in the event of a labour dispute. The impact of this risk is high for data subjects, especially if the administrators would keep the Intune log files for longer than the standard 30-day period, and would export them to an Intune data warehouse, and/or unlock them with PowerBI. This risk assessment also takes account of the fact that the data subjects have no control over the use of the digital traces they leave behind in the Intune and Azure AD log files, because they are obliged to make use of Intune.

The European DPAs stress the importance of providing good information to employees when using MDM in their opinion on workplace data processing: *"Employees whose devices are enrolled in MDM services must also be fully informed as to what tracking is taking place, and what consequences this has for them."*[183]

The government organisations can not process location data from the devices if they limit the deployment to self-managed personal or corporate devices. However, if they would choose fully supervised deployment, they should take specific measure to protect employees against the possibility of unwarranted tracking of their location data, a main concern of the DPAs.

Government organisations should set rules for possible further processing of the log-in and log-out data and other personal data from the log files. Provided that government organisations follow the recommendations of this report to provide data subjects with more information about the nature and extent of the data processing via Intune, the likelihood of occurrence of this risk can be qualified as low.

Given the low probability that the risk will occur, despite the potentially high impact on individuals, the risk of a chilling effect on the employees through the use of Intune is low.

16.2.3 Lack of purpose limitation Company Portal app

Contrary to the privacy amendment, Microsoft considers itself the data controller, which means it allows itself to process the data for seventeen purposes. Although the inspection of the technical data flow shows that Microsoft does not collect sensitive or content data via the telemetry from the app or via the debug log from the device, Microsoft's role nevertheless poses a risk to data subjects, because the data flow is dynamic and can be changed *on the fly*.

Microsoft mentions the 'sharing of data' as one of the purposes of the processing. Microsoft's assertion that it does not sell any data (see Figure 29 in Section 4.2) is therefore irrelevant to the assessment of the risks for data subjects. Microsoft explicitly mentions the possibility that it can base the advertisements on usage data. On the basis of its privacy statement, Microsoft could therefore display targeted advertisements in Microsoft products, (partly) on the basis of information it obtains from the Company Portal app.

[183] Article 29 Data Protection Working Party, WP 249, Opinion 2/2017 on data processing at work, 8 June 2017, URL: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=54650 , p. 20.

The administrators of government organisations do not have the technical ability to centrally prevent the sending of telemetry and the keeping of a debug log in the Company Portal app. There is only a Block option of devices with iOS and iPadOS. Therefore, the administrators can only encourage employees to disable data sharing via telemetry individually, via the app. Because the use of the Intune Company Portal app is mandatory, while government organisations are unable to block the sending of telemetry centrally for all devices, they are joint controller with Microsoft. Because there is no joint controller contract, there is a real chance that data subjects will not know where and how to exercise their data protection rights.

Due to the lack of technical management options and because Microsoft considers itself to be controller, the likelihood that the risks of loss of control, loss of confidentiality and unlawful (further) processing will occur is 100%. Due to the relatively innocent content and the relatively small number of diagnostic messages from the Intune Company Portal app, the impact of this lack of control for data subjects is low, based on the current nature and content of the telemetry data and the debug logs. Because the impact on individuals is low, the privacy risk for individuals is low.

16.2.4 Lack of transparency of diagnostic data Company Portal app

Microsoft publishes a lot of technical information about the nature and content of the different Intune and Azure AD log files. Microsoft informs users via the Company Portal app with a bullet list about the categories of data administrators can and cannot collect via Intune (see Figures 6 and 7). However, Microsoft does not provide any information about the diagnostic personal data it processes itself through the Company Portal app and the debug log. Although Microsoft offers an opt-out option to data subjects for sending telemetry via the app, this opt-out cannot compensate for the lack of transparency, because data subjects are not even aware that telemetry is being sent and they are not being asked whether they accept this type of data processing during the installation of the app. They are therefore effectively unable to exercise their rights.

The data protection supervisors in the EU write in their opinion about monitoring in the workplace:
"*Owing to the capabilities of such technologies, employees may not be aware of what personal data are being processed and for which purposes, whilst it is also possible that they are not even aware of the existence of the monitoring technology itself.*"[184]

Microsoft does not provide information about the existence and content of the telemetry messages in technical language for admins. Neither admins nor data subjects are able to view the data flow in readable form, because Microsoft does not provide a Data Viewer tool, as is the case with the telemetry from Office 365 and Windows 10.

Because Microsoft does not publish documentation and data subjects cannot check the data flow themselves, they cannot know what diagnostic data Microsoft is processing about them via the Intune Company Portal app.

[184] Article 29 Data Protection Working Party, WP 249, Opinion 2/2017 on data processing at work, 8 June 2017, URL: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=54650, p. 11,

As a result, government organisations, as joint controllers with Microsoft, are unable to determine whether the processing is lawful and insufficiently able to adequately inform their employees.
Due to the relatively innocent content of the telemetry data and the debug logs, as currently observed, the impact of this lack of control for data subjects is low.

16.2.5 Transfer of diagnostic personal data to the U.S.

As explained in Section 7 of this report (*Transfer of personal data outside of the EU*), the transfer of diagnostic personal data to a country outside the EU in itself poses a risk for data subjects. Microsoft transfers the app's telemetry data and debugging files to servers in the United States. Microsoft indicates that it processes the Intune and Azure AD log files in principle in the same region where the customer content are processed. "*Log files are (…) originally created and stored in Azure storage in the data center where Azure AD service runs.*" But then these log files are scrubbed and stored in Microsoft's long-term database in the U.S.[185] Microsoft also writes that the data processed with multi factor authentication are always processed exclusively in two data centers in the U.S., in Iowa and in California.[186] Microsoft writes: "*All two-factor authentication using phone calls or SMS originate from U.S. datacenters and are also routed by global providers*."[187] This also applies to digital push messages in the Authenticator app.

The technical research shows that the content of the Intune log files, the Azure AD log files and the data from the Company Portal app are relatively harmless. For this reason, the impact on data subjects of unlawful processing of these personal data is, in principle, limited. However, the impact is strongly related to the length of the retention period.

The retention periods of diagnostic data at Microsoft are not clear. A risk of this is that data subjects cannot exercise their rights to request access or, for example, to have obsolete data deleted. This applies to at least one specific Azure AD security log file and to the telemetry data from the Company Portal app.

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

While Microsoft undertakes to ensure a uniformly high standard of protection, this protection cannot be guaranteed against government interference of third countries outside the EEA. Therefore, there is a non-negligible risk that information held by Microsoft in a data centre in a third country can be accessed by local governments, through a hack or by forcing an administrator to do so.
With regard to the risk of hacks through rogue administrators or hostile state actors, *on-premise* local hosting does not offer better guarantees for a timely detection of new risks, and implementation and monitoring of up-to-date security measures. Microsoft has a very large number of dedicated security staff and

[185] Public Microsoft whitepaper, Ramiro Calderon, Azure Active Directory Data Security Considerations, Version: 1.01, Published: June 2018, URL: https://aka.ms/aaddatawhitepaper
[186] Microsoft, Identity data storage for European customers in Azure Active Directory, 4 March 2019, URL: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-data-storage-eu
[187] Idem.

controls the legitimacy of access to personal data with technical and organisational measures that are regularly audited.

Microsoft transfers the log files on the use of the Intune and Azure AD cloud services to the U.S. as a data processor, based on the EU Standard Contractual Clauses. The telemetry data from the Intune Company Portal app are transferred on the basis of the EU-U.S. Privacy Shield contract. Microsoft self-certified under this regime.[188] Although both of these transfer mechanisms are legally valid, and approved by the European Commission, there is serious doubt about the future validity of these instruments with regard to transfers to the USA. The European Court of Justice was asked to decide whether this agreement and these clauses offer sufficient mitigation for the risks of extensive surveillance in the USA as brought to light by whistle blower Edward Snowden, including the risk of data being observed in transit to the USA.[189]

These risks (of access to personal data by the U.S. law enforcement and security services) do not only apply to content stored on Microsoft's cloud servers such as employee account names, but also to diagnostic data, and they apply worldwide. Although Microsoft provides a guarantee regarding the storage of content in data centers in the Netherlands and Ireland, North American courts reserve the right to claim access to these data under the USA CLOUD Act. This Act effectively extends the jurisdiction of the North American courts to all data under the supervision of North American companies, even if the data are stored in data centers outside the territory of the United States.

Microsoft publishes a report on the number of requests made by law enforcement agencies twice a year. Microsoft explains that it receives very few requests/claims about the Enterprise business customers of cloud services.[190] However, according to the different reports about the second half of 2018 and the first half of 2019, the number of requests increased: from 22 to 42 approved claims for data from

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

[189] In case C-311/18 the European Court of Justice will take the facts into consideration established in the case of Max Schrems versus the Irish DPC. The court hearing took place on 9 July 2019. Advocate General Henrik Saugmandsgaard Øe has published his Opinion on 19 December 2019. The other procedure is Case T-738/16. This request was filed by the French non-governmental digital rights organisation La Quadrature du Net on 9 December 2016. The hearing at the court was scheduled for 1 and 2 July 2019 but has been postponed in order to allow the court to first decide about the Schrems-2 case.

[190] Microsoft writes in her transparency report about requests of law enforcement authorities, in reply to the question 'How many enterprise cloud customers are impacted by law enforcement requests': *In the first half of 2019, Microsoft received 74 requests from law enforcement around the world for accounts associated with enterprise cloud customers. In 32 cases, these requests were rejected, withdrawn, no data, or law enforcement was successfully redirected to the customer. In 42 cases, Microsoft was compelled to provide responsive information: 22 of these cases required the disclosure of some customer content and in 20 of the cases we were compelled to disclose non-content information only. Of the 22 instances that required disclosure of content data, 15 of those requests were associated with U.S. law enforcement.*
In the second half of 2018, Microsoft received 61 requests for data of Enterprise customers. 39 requests were rejected or withdrawn.
In answer to the question about the effects of the CLOUD Act, Microsoft writes: "*In the first half of 2019, Microsoft received 4,860 legal demands for consumer data from law enforcement in the United States. Of those, 126 warrants sought content data which was stored outside of the United States. In the same time frame, Microsoft received 43 legal demands from law enforcement in the United States for commercial enterprise customers who purchased more than 50 seats. Of those demands, 1 warrant resulted in disclosure of content data related to a non-US enterprise customer whose data was stored outside of the United States.*"
https://www.microsoft.com/en-us/corporate-responsibility/lerr/.

Enterprise customers. This concerned 20 claims for metadata and 22 for content data. Fifteen of these requests came from the U.S. Microsoft does not disclose the origin of the remaining requests.[191]
Under the OST, Microsoft is contractually bound to inform its customers in principle when it receives such a request. Microsoft explained to SLM Rijk that there is a high legal threshold for requests about which it is not allowed to inform its business customers (because Microsoft would then be obliged to remain silent).

As quoted in Section 4.4 Microsoft explains in the OST that it will not disclose Processed Data to law enforcement unless required by law and will try to redirect the request to the data controller/customer. *"If compelled to disclose Processed Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so."*[192]

Although Microsoft also reports twice a year on law enforcement and security orders, through FISA orders, these publications only contain estimates of totals, not broken down by country or type of customer (consumer or business).[193]

Since the introduction of the new OST and DPA in January 2020, Microsoft's privacy assurances about forwarding prospecting requests also apply to telemetry data and system generated logs when Microsoft acts as data processor. These guarantees do not apply to telemetry data from apps and installed software. Though the technical inspection of the telemetry data and the debug log show that Microsoft collects a limited amount of data, without sensitive content, Microsoft as data controller feels free to share personal information 'in good faith'. Microsoft states that it may disclose personal information, including content when it has a good faith belief that it is necessary to respond to valid legal requests from law enforcement.

Microsoft writes: "*Finally, 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. "*[194]

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

As assessed by the European Data Protection Board (EDPB) and the EDPS in their joint opinion to the LIBE Committee of the European Parliament on the CLOUD Act, transfers of personal data must comply with Articles 6 (principles) and 49

[191] Microsoft, Microsoft Law Enforcement Requests Report, URL: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report. For all European consumer clients Microsoft has received 24.175 requests, with regard to 43.727 users. Of those requests, Microsoft rejected 26.76% and was unable to find data in 14.46% of the cases. Compared to requests relating to residential and small business users, the number of requests relating to large business customers is therefore still low, (0.3%).
[192] Idem.
[193] Microsoft, U.S. National Security Orders Report, URL: https://www.microsoft.com/en-us/corporate-responsibility/fisa . For example, in the second half of 2018, Microsoft received between 0 – 499 orders for content, relating to 13,500 - 13,999 accounts.
[194] Microsoft privacy statement, last updated February 2020.

(exceptions allowing transfers) of the GDPR. If an order is issued on the basis of the U.S. CLOUD Act, the transfer can only be lawful if it is based on an international treaty. The DPAs stress the need for new MLATs (mutual legal assistance treaties) and the need to negotiate an international treaty between the EU and the U.S. on cross-border access to electronic evidence for judicial cooperation in criminal matters.

It is up to the European Court of Justice to assess the validity of the SCC for the transfer of data from the EEA to the U.S., and up to the European Commission to negotiate a new mutual legal assistance contract with the U.S., as well as a treaty on access for law enforcement services.

In sum, the use of Intune MDM and MAM, in combination with the Azure AD and the Intune Company Portal app, if the government organisations deploy Intune as tested for self-managed devices, results in a low risk of unlawful access to personal data by U.S. courts or authorities, while the consequences for data subjects can vary from low to very serious. This results in a low risk for data subjects.

16.3 Summary of risks

These circumstances lead to the following five low risks in terms of data protection:

1. Unauthorised access to administrators' settings: loss of control, confidentiality and unauthorised further processing
2. Chilling effect personnel monitoring system: loss of confidentiality
3. Lack of purpose limitation Company Portal app: loss of control, loss of confidentiality, re-identification of pseudonymised data and unlawful (further) processing
4. Lack of transparency in diagnostic data Company Portal app: obstacle exercise of data subjects' rights, loss of control, loss of confidentiality, reidentification of pseudonymised data and unlawful (further) processing
5. Transfer of diagnostic personal data to the U.S.: loss of control, risks of loss of confidentiality, re-identification of pseudonymised data and unlawful (further) processing

Based on the ICO model, this results in the following matrix:[195]

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

Part D. Risk mitigating measures

This part of the DPIA discusses what additional measures Microsoft and government organisations can take to eliminate or reduce the low risks.

17. Risk mitigating measures

Section 16 concludes that the processing of personal data by government organisations of self managed devices through Microsoft Intune MDM and MAM, in combination with the Azure AD and the use of the Company Portal app, leads to five low risks for data subjects. Government organisations can largely mitigate these five low risks themselves through a number of technical and organisational measures. Additionally, SLM Rijk should continue to negotiate with Microsoft to ensure that Microsoft will correctly apply the privacy amendment, e.g. act only as a processor in relation to the Company Portal app, and will implement technical improvements in the areas of privacy by design and data minimisation.

Because the research was done on a tenant with a combination of MDM and MAM, it is not possible to make a technical distinction in this DPIA between log files relating to MDM and log files relating to MAM. Therefore, it is not possible to distinguish between measures that only apply to MDM and measures that only apply to MAM.

The main difference is that when using MAM without MDM, i.e. *without enrolment*, system administrators have less control over employees' self-managed devices, and therefore the risks of covert conversion to a corporate device cannot occur. Therefore, to fulfil their transparency obligations, organisations that use MAM-WE have to provide different information to their employees about the risks and the nature and scope of the processing.

[195] 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/

The measures in the table are explained point by point below, divided into measures that the government organisations can take themselves and measures that Microsoft should take, encouraged by SLM Rijk.

Low risks	Measures government organisations	Measures Microsoft (via SLM Rijk)
Unauthorised access by organisations' system administrators to personal data on personal devices	Explicit prohibition to change the status of devices from personal to corporate without information and prior warnings	Privacy by default: the Company Portal app must always provide an active warning to the user in the event of a change in management status, or actively request consent from data subjects
	Logging & systematic monitoring of the behaviour of system administrators in accordance with specific policy, check measures such as a certificate of conduct (VOG)	
Risk that Intune is perceived as a personnel monitoring system: Chilling effect employees	Expand the internal privacy policy with rules for logging and purposes for access	Data minimisation: the default setting at Microsoft is a retention period of one year for the Intune audit log files, while the administrators may only need a shorter retention period. The administrators must be able to determine the period themselves
	Create internal privacy page about Intune and explain what the organisation will and won't do with Intune MDM and MAM and the Azure AD	
	Check the available functionalities and/or use of full device management capabilities against internal privacy policy and authorisation matrix	
Lack of purpose limitation data processing via the Company Portal app	Advise employees to turn off both the telemetry flow and the debug log and put the telemetry level in Windows 10 Enterprise on Basis or Security to minimise data traffic to Microsoft in its role as the controller	Act as processor for the Company Portal app: all necessary Intune processing in accordance with the privacy amendment
		Privacy by default: offer administrators the option to centrally disable telemetry and debug log via the Company Portal app
Lack of transparency diagnostic data Company Portal app	Supplement information from Microsoft on internal privacy page about the types of data with factual findings from this DPIA	Publish information about the nature of the data collected through the Company Portal app and debug log
		Provide data viewer tool to view traffic from the Company Portal app

Transfer of personal diagnostic data to the U.S.	Follow recommendations SLM Rijk following case law of EU Court of Justice	Consider processing of personal data Azure AD exclusively in the EU, in particular MFA
		Data minimisation by allowing administrators to choose retention time Intune log files and the ability to centrally disable telemetry from the Company Portal app.
		Provide data viewer tool to view traffic from the Company Portal app

17.1 Measures government organisations

In order to further mitigate low risks for data subjects, government organisations themselves can take the following five measures:

1. Prohibit status change of devices from personal to corporate

To avoid the risk of system administrators covertly changing the status of an employee's device via Intune MDM, and thus gaining access to all installed apps and (only on iOS) to the full phone number, government organisations should explicitly prohibit administrators from changing the status of self-managed devices.

2. Systematic monitoring of system administrators' behaviour in accordance with existing policies

Government organisations cannot suffice with a policy rule that administrators may not change the status of self-managed devices. They must develop a policy to systematically check the Intune logs of system administrators' behaviour, in order to be able to detect and, above all, prevent abuse. In order to limit employee access to the information necessary for their role, organisations can make use of Intune's detailed role-based access management (RBAC) capabilities.[196] Azure AD Privileged Identity Management allows organisations to keep logs of system administrators' activities in Intune: the login history, changes to management tasks, and alerts on access to privileged roles. In addition, government organisations are required under BIO rules to require system administrators to have a certificate of conduct.

3. Turn off telemetry and debug log in Intune Company Portal app and telemetry in Windows 10

To reduce the risks of Microsoft processing telemetry data and the debug logs from the Intune Enterprise Portal app, government organisations can advise employees to turn off the telemetry flow and the debug log. The necessary steps are described in Section 3.1 (*Privacy Choices Intune and Azure AD*). The administrators of Windows 10 Enterprise can set the telemetry level of Windows 10 to the lowest Security level to prevent the processing of telemetry data.

4. Provide detailed information on an Intune privacy page

[196] Microsoft, Role-based access control (RBAC) with Microsoft Intune, 22 March 2019, URL: https://docs.microsoft.com/en-gb/intune/fundamentals/role-based-access-control

As recommended in Section 1.2.2 (*Android*), government organisations should create an internal privacy portal with dedicated information about the specific deployment of Intune, at least with a FAQ with an explanation what the administrators can and cannot see.

Article 12 of the GDPR requires government organisations, whether joint controllers with Microsoft or independently, to publish in plain language, in easily accessible, comprehensible and succinct information, inter alia, on their identity as controllers, the different purposes of data processing via MAM and MDM, the retention periods, and how data subjects can exercise their rights.

To reduce the risks of Microsoft's lack of transparency and to not prevent unnecessary fear among employees about Intune's ability to monitor their behaviour, government organisations can supplement the separate explanation on the Privacy Portal with texts from this DPIA about:

1. The most important differences between Intune MDM and MAM (see the summary and introduction on the scope of this DPIA)
2. The policy of government organisations to use Intune to a very limited extent (see the text in the introduction about the processing operations that are outside the scope of this DPIA);
3. The types of personal data processed (see Sections 2.2, 2.3 and 2.4 of this DPIA);
4. The purposes of the processing (different depending on whether Microsoft acts as processor or controller (see Sections 4.1, 4.2 and 4.3 of this DPIA);
5. The rights of data subjects (see Section 15 of this DPIA).

Currently, Microsoft shows two bullet lists via the app, about data that Microsoft does and does not collect. This explanation is too brief. There is no general explanation about Intune, and the differences between MDM and MAM. Since February 2019, Microsoft published extensive information about the diagnostic data that system administrators can see via the various log files about the use of Intune MAM and MDM on the various platforms (see Section 2.2 of this report, *Three types of Intune log files*). Microsoft expects the system administrators, as controllers, to inform employees what data they are collecting. The advice is to publish the following list of personal data on the dedication information page, with a hyperlink to Microsoft's detailed information.

- Device model, such as Google Pixel
- Device manufacturer, such as Microsoft
- Operating system and version, such as iOS 12.0.1
- Inventory and names of the Microsoft apps managed with Intune, such as Microsoft Word (MAM only)
- Owner of the device
- Device name
- Serial number of device
- UDID, IMEI, MEID and Intune Device ID (unique device identifiers)
- Total available and free storage space on the device
- Date of last contact with Intune
- The last four digits of the phone number of the device.
- userID
- e-mail address
- e-mail alias

It follows from the technical inspection that devices with Windows 10 Enterprise are always installed as corporate devices. Government organisations should inform

employees that as a result, the names of a large proportion of the (pre)installed Microsoft apps on Windows 10 Enterprise are always visible to Microsoft and the system administrators. They must also inform employees of other platforms when the devices are registered as 'corporate', and what the privacy consequences of this are. Especially iOS users need to know that administrators can see their full phone number and all apps installed through the app store.

There is also a lack of information about the diagnostic personal data Microsoft processes through the Company Portal app and the debug log. Microsoft does not provide information about the existence and content of telemetry messages in technical language for admins. Neither admins nor data subjects are able to view the data stream in readable form, because Microsoft does not provide a Data Viewer tool, as it does for the telemetry from Office 365 and Windows 10. Government organisations can compensate for this lack of transparency by adding the tables with identifiers found in this report to the information on their own privacy page.

Because government organisations are joint controllers with Microsoft for data processing via the Intune Company Portal app, they must inform employees via their privacy page about their right to request access from the government organisation and lodge a complaint, internally with the Data Protection Officer and externally with the Dutch DPA.

In the installation flow of the Company Portal app, Microsoft asks for a number of consents. The information about these requests can also be improved.

- The app requests consent to make phone calls. The wording is unfortunate, because the app does not want to make phone calls but only needs access to the IMEI of the device.
- In Android, the app asks consent to turn off the camera. This should only be asked if the government organisations want to use this functionality.
- There is no explanation in the manual how users can see the ownership type in Windows 10.
- Microsoft does not ask for consent, or offer an opt-out, for the collection of telemetry data and debug logs.

5. Review initial deployment and future expansion of Intune processing against internal privacy policy and conduct DPIA when necessary

Both during the initial enrolment, as well as during future expansion of the use of Intune's features, the organisations should balance the need for information security purposes against the possible privacy risks for employees. The organisations should check new logging possibilities against their internal privacy policy, and adjust the specific Azure AD and Intune authorisation matrix accordingly.

17.2 Measures Microsoft (via SLM Rijk)

In order to further mitigate the low risks for data subjects, Microsoft could make the following three legal and five technical improvements:

1. Ensure purpose limitation when using the Company Portal app;
2. Have audits conducted on purpose limitation, anonymisation, retention periods, and Azure AD logs;
3. Legal guarantees for data minimisation and transparency;
4. Privacy by default: send a clear warning to users in case of status change;
5. Allow system administrators to determine the retention period of Intune log files;
6. Create a central opt-out for administrators for telemetry and debug logs;
7. View telemetry data via Data Viewer Tool;
8. Process Azure AD data only in European cloud, especially MFA

Irrespective of this, SLM Rijk is preparing for the consequences of the future ruling of the European Court of Justice on the risks of transfer of personal data to the U.S. If the Court of Justice decides that the Standard Contractual Clauses do not constitute a valid basis for transfer, SLM Rijk will consult with other government cloud services vendor managers and with Microsoft about the solutions that Microsoft can offer.

1. Ensuring purpose limitation when using Company Portal app

Microsoft still considers itself as data controller for the Intune Company Portal app. On the basis of the (last available) privacy statement of February 2020 (which users can read via a hyperlink when downloading the app from the app store), Microsoft allows itself to process the data for seventeen purposes. Although the inspection of the technical data flow shows that Microsoft does not collect sensitive or content-related data via the telemetry from the app, Microsoft's role as controller does pose a risk to data subjects, also because the data flow is dynamic. In order to further reduce this low risk, SLM Rijk should strive to obtain Microsoft’s commitment that will only process the data from the Company Portal app for those purposes for which government organisations have a legal ground, as agreed upon in the privacy amendment. Microsoft should always act as data processor for the Intune Company Portal app, not only in cases where an employee uses the Azure AD, but also in other cases where government organisations want to use Intune MAM without enrolment (i.e. without registering with Intune MDM) in combination with a local Azure AD. Microsoft’s current commitment in relation to similar role shortcomings in the Office apps, is insufficient. As quoted in Section 4.2, Microsoft only provides guarantees for the data that are sent from the apps to Microsoft’s online services, not with regard to the telemetry collected from the app.

2. Collaborate with audits on purpose limitation, anonymisation, retention periods and Azure AD logs

SLM Rijk will verify Microsoft’s compliance with the strict purpose limitation, in particular with regard to diagnostic data, including telemetry messages from installed software and apps, and system-generated logs of events on Microsoft's own servers. Because Microsoft does not offer administrators and data subjects access to at least one specific system generated log file about the Azure AD that Microsoft processes for its own security purposes, and because Microsoft keeps these data in a pseudonymised form in Cosmos for a long time (one year or as much longer as necessary), this DPIA recommends that SLM Rijk should audit the contents of this log file.

It is recommended to also check the contents of other log files that Microsoft processes for its own purposes, and check whether these processing operations are compatible with Microsoft's role as data processor, and whether these processing operations are necessary to protect the legitimate interest of government organisations in protecting the service against unauthorised access.

The quality of the anonymisation of Azure AD and Intune log files should also be verified, whether Microsoft indeed follows the technical guidelines for anonymisation of DPAs in the EU, as laid down in the WP216 Opinion. Microsoft describes that the Azure AD log files contain usernames but that it removes these personal data from the log files (scrubbing) before processing the data in its machine learning systems for general analysis. As described in Section 8.2, anonymisation is a complex and dynamic form of data processing. As long as there is a realistic possibility to re-identify the pseudonymised data, the stored data cannot be considered anonymous.

Finally, the factual retention periods should be verified. In a published audit report about Azure, the auditor notes that Microsoft engineers reassess the numbers and types of events every six months. The data from the specifically mentioned system generated Azure AD log are stored for 30 to 90 days in the Geneva monitoring tool, and stored in the Cosmos database for one year or as much longer as necessary (as needed). [197]

SLM Rijk collaborates with other large-scale public sector vendor managers of cloud services in Europe, in order to divide tasks and achieve a harmonised set of rules for cloud providers.

3. Legal guarantees for data minimisation and transparency

Intune is a dynamic product. Transparency is currently lacking, especially when it comes to the processing of the two types of diagnostic data from the Company Portal app: telemetry data and the debug log. Deeply hidden in a multitude of information about Intune, Microsoft provides one very concise explanation under the heading "*How to turn off Microsoft data collection'. In it, Microsoft writes: "Microsoft automatically collects certain data about our products and services. We do this to improve the reliability and performance of our products, including the Company Portal app. Even though this data is anonymised, some users may not feel comfortable with this collection.*" [198]

Microsoft does explain how users can disable data sharing in the app, but only for the telemetry data, not for the debug logs. That information can only be found after a user has become aware that this processing exists. But the nature and extent of the data processing of log files in Cosmos is also completely opaque. In order to prevent unexpected new risks caused by future processing possibilities in Intune for data subjects, SLM Rijk will continue to negotiate with Microsoft to provide a legal guarantee of data minimisation and transparency regarding the content of data processing.

4. Privacy by default: warning to users in case of status change

[197] BSI Assessment report on compliance standard ISO/IEC 27001:2013 and ISO IEC 27018:2014 by Microsoft Azure, published on 23 August 2018, p. 13.
[198] Microsoft, Turn off Microsoft usage data collection [on Android], 19 April 2019, URL: https://docs.microsoft.com/en-gb/intune-user-help/turn-off-microsoft-usage-data-collection-android

This DPIA shows that Microsoft does not clearly inform data subjects when a system administrator changes the device status in MDM. Microsoft must ensure that the Company Portal app always gives an active warning to the user when the management status changes, or that the app actively requests for consent from the data subjects. Microsoft should also adapt the text of the current notice to administrators. That notice makes it appear as if data subjects can see the status change, and that is only the case if a data subject looks in the Company Portal app by chance.

5. System administrators must determine the retention period for Intune log files

Government organisations must be able to determine the retention period for the Intune log files. However, Microsoft saves the audit log files for one year by default. Microsoft should give the controllers/customers the option to determine the retention period themselves. After all, the retention period is an important 'means' of data processing, and only controllers may decide how long data are to be retained.

6. Providing insight into telemetry data via Data Viewer Tool

Currently, there is no easy way to view the data flow of the Company Portal app in readable form. The traffic was intercepted, but only the traffic from macOS and iOS could be analysed, and most recently, only from iOS. The traffic from Android could not be decoded and the traffic from Windows not distinguished. Microsoft must make the Data Viewer Tool available for analysis of this traffic, in addition to publishing extensive documentation to allow users to compare the results they found. This measure seems unnecessary if there would be a central switch-off button, but remains very important when Microsoft only acts as data processor for the app. With the Data Viewer tool, Microsoft can demonstrate that the collected data are indeed necessary for the three legitimate processing purposes.

7. Central option to turn off telemetry and debug log for administrators

The system administrators can now only point users to the individual opt-out options for telemetry and the debug log from the Company Portal app. This does not provide sufficient assurance to government organisations, as joint controllers with Microsoft, that they have a legal basis for processing. They therefore need to be able to block the two processing operations centrally, via a group policy or a modified version of the app.

8. Processing Azure AD data only in the EU

In order to further mitigate the low risks for data subjects, Microsoft should offer the full Azure AD service, including MFA, from the European data centres. This could also be an important preparation for GDPR compliance, following a possible negative opinion of the European Court of Justice on the legitimacy of the current transfer instruments of the European Commission.

17.3 Conclusions and advice

This DPIA concludes that government organisations can deploy Intune for self-managed devices without high data protection risks for the government employees. However, there are five low risks. Two of those risks are related to the mandatory use of the Intune Company Portal app, two other risks are related to the nature of registering information about employees' devices, and the last risk stems from the fact that Intune is a cloud service provided by Microsoft, a U.S.-based provider.

The assessment that the data protections are low, and not high, is based on the relatively innocent nature of the diagnostic data: no content data or other data of a sensitive nature, nor detailed records of individual behaviour. Additionally, government organisations can take effective measures to prevent the collection of sensitive data from the devices.

This DPIA recommends 8 measures Microsoft should take. SLM Rijk will continue to negotiate with Microsoft to ensure that Microsoft will only process the data that it collects via the app as a data processor and under no circumstances as the controller.

This DPIA focusses on self-managed devices, either as personal or corporate devices. The actual risks depend on the factual implementation per organisation. An organisation can also use Intune to manage corporate devices in fully supervised mode. This type of enrolment allows for greater access to user activities and behaviour. Each government organisation should therefore conduct its own DPIA, based on this umbrella DPIA, to determine what measures are necessary to enforce compliance with its information security policy, without causing high data protection risks for the government employees.

Other measures government organisations can take to mitigate the low risks are:

1. Advise employees to turn off telemetry and debug logs in the Company Portal app
2. Add an explicit policy rule to the existing internal privacy policy that administrators may not change the status without informing and alerting the user
3. Systematically check the log files about the administrators' behaviour, in accordance with existing policies
4. Ensure administrators have a valid certificate of conduct.
5. Expand the internal privacy information with an explanation of the purposes and categories of data collected through Intune MDM and MAM, what the system administrators can and cannot see on the self-managed devices.

Measures Microsoft

This DPIA was conducted between September 2019 and April 2020 and contains outcomes with respect to processing in connection with the use of Microsoft Intune as at 31 March 2020. SLM Rijk provided Microsoft with the DPIA findings upon completion of this DPIA. Between April and June 2020, SLM Rijk and Microsoft agreed upon measures to mitigate two of the five low protection risks ultimately in the fall of 2020.

These measures are:

1. Microsoft will only act as data processor for the Intune Company Portal App, with the exception of processing for Microsoft’s own legitimate business purposes, and all processing will be in accordance with the privacy amendment.

2. Microsoft will publish documentation about the nature of the data collected through the Company Portal App and debug logs. This documentation must provide customers with a good understanding of the data that Microsoft collects.

These measures will have to be implemented at the latest in the fall of 2020. SLM Rijk will publish an update about the implementation progress early in 2021.

Appendix 1: Executed test scenarios per platform

Checklist in advance
Privacy Company executed these test scenarios on the four different platforms in September and October 2019. Some of the tests were repeated in March 2020.

The research was conducted on the following devices.

System and OS September/October 2019	System and OS March 2020
iPhone X with iOS 12.4	iPhone XS Max with iOS 13.3.1[199]
Google Pixel with Android 9	Google Pixel 3 XL with Android version 10 build QQ1A.200205.002[200]
Dell laptop with Windows 10 Enterprise version 10.0.18362.30.19h1_release	Dell Latitude Windows 10 Enterprise 1803, build 17134.1304
Macbook with macOS 10.14.6	Macbook with macOS 10.15.3

The test scenarios were largely executed in the same way on the four platforms. Differences in the execution are mentioned below.

The test scenarios on all devices started without installation of the Company Portal app and without registration in Intune. The two user accounts were registered in the Azure AD prior to testing, with a corresponding Intune Policy. This policy includes an obligation for devices to use disk encryption. Disk encryption was disabled on all devices except iOS. Prior to the testing, a test file containing non-functional malware[201] was stored on the accounts' OneDrive.

Test scenarios
The test equipment was registered in the Intune tenant. The Company Portal app was installed on three platforms. Only in Windows 10 Enterprise the Company Portal app was not used. Instead, the built-in software in the operating system was used to manage the laptop. It was then checked whether disk encryption was enforced on all devices. This was the case for all devices.

OneDrive and Office 365 were then installed on all devices. On Android and iOS this was done via the App Stores and on Windows and macOS it was done via the online Office environment in the browser. A third-party app was also installed via the app stores of the various platforms. The app was chosen to present user preferences and indicate data of a sensitive feature. On iOS a pregnancy app was installed, on Android the FitBit app, on Windows the Pillbox app and on macOS the Diabetespal app. On all platforms the standard browser (Edge on Windows, Safari on macOS and iOS and Chrome on Android) was used to visit the website https://www.amc.nl/ and a page of the outpatient cardiology clinic was looked up. The EICAR test malware was then downloaded from the OneDrive app and e-mailed to the other test account via the Outlook app.

The test was completed by having the organisation's administrator remotely erase the devices and then perform a DSR on the test accounts.

[199] Privacy Company tested Company Portal for iOS version 4.3.1.
[200] Privacy Company tested Company Portal for Android version 5.0.4700.0.
[201] EICAR testfile https://www.eicar.org/?page_id=3950