#### Technical verification report Microsoft <u>Defender</u> 365 for Enterprise and for Education

Version 1.0

Date

22 May 2023

# Colophon

Technical verification report by	Ministry of Justice and Security, Strategic Vendor Management Microsoft, Google and AWS (SLM Rijk)	
	Turfmarkt 147 2511 DP The Hague PO Box 20301 2500 EH The Hague www.rijksoverheid.nl/jenv	
Contact	Henrique Barnard E h.m.barnard@minjenv.nl T 070 370 79 11	
Project Name	Technical verification report Microsoft Defender 365	
Authors	Privacy Company Sjoera Nas and Floor Terra, senior advisors https://www.privacycompany.eu/	

# Change log

Version	Date	Summary of input
0.1	4 November 2021	First Privacy Company internal rough draft
0.2	16 June 2022	Completed draft, with tech input after DSAR and audit log results
0.3	1 May 2023	Modified draft after input Microsoft and public clarifications - with track changes
0.4	22 May 2023	Interim version with more input Microsoft with track changes
0.5	22 May 2023	Clean version

## CONTENTS

Colofon	3
Change log Figures Tables	1 3 4
Summary	5
<ol> <li>Introduction         <ol> <li>Previous DPIAs on Microsoft Office 365</li> <li>Scope of this report: Microsoft 365 Defender</li> <li>Test methodology</li> <li>About Microsoft 365 Defender</li> <li>Different resources in Defender 365 portal</li> </ol> </li> </ol>	8 9 9 11 12 18
2. Verification questions	28
<ol> <li>Detection of malicious files, apps and URLs</li> <li>Facts</li> <li>Technical findings</li> <li>Assessment</li> <li>Remedies</li> </ol>	28 29 29 33 34
<ul> <li>4. Detection of suspicious logins in the Azure AD</li> <li>4.1 Facts</li> <li>4.2 Technical findings</li> <li>4.3 Assessment</li> <li>4.4 Remedies</li> </ul>	35 35 36 39 39
<ol> <li>Data minimisation options</li> <li>5.1 Facts</li> <li>5.2 Assessment</li> <li>5.3 Remedies</li> </ol>	40 40 41 42
<ul> <li>6. Traffic to third parties</li> <li>6.1 Facts</li> <li>6.2 Technical findings</li> <li>6.3 Assessment</li> <li>6.4 Remedies</li> </ul>	42 42 43 51 53
<ul> <li>7. Learnings from security incidents</li> <li>7.1 Facts</li> <li>7.2 Technical findings</li> <li>7.3 Assessment</li> <li>7.4 Remedies</li> </ul>	53 53 54 54 56
<ul> <li>8. Risk profiles</li> <li>8.1 Facts</li> <li>8.2 Technical findings</li> <li>8.3 Assessment</li> <li>8.4 Remedies</li> </ul>	56 56 58 58 58
<ul> <li>9. Quality of public information</li> <li>9.1 Facts</li> <li>9.2 Technical findings</li> <li>9.3 Assessment</li> <li>9.4 Remedies</li> </ul>	59 59 61 61 62

10. Data Subject Access	62
10.1 Facts	62
10.2 Technical findings	64
10.3 Assessment	71
10.4 Remedies	74
11. Transfer risks	74
11.1 Facts	74
11.2 Technical findings	76
11.3 Assessment	76
11.4 Remedies	77

#### Figures

Figure 1:Illustration Microsoft tools in Microsoft 365 Defender	10
Figure 2: Microsoft graphic Core Defender services	13
Figure 3: Microsoft illustration scale of Defender	13
Figure 4: Collated screenshots of Microsoft 365 Defender Homepage	14
Figure 5: Microsoft illustration of EOP filtering	15
Figure 6: Illustration Microsoft Defender for Endpoint	17
Figure 7: Microsoft illustration of Cloud Apps Architecture	18
Figure 8: Screenshot Microsoft Device Inventory	19
Figure 9: Screenshot Microsoft Threat & Vulnerability Management dashboard	20
Figure 10: Incidents & alerts	20
Figure 11: Screenshot Microsoft alert about suspicious domain	21
Figure 12: (Global) threat analytics	22
Figure 13: Explorer (mail security incidents)	22
Figure 14: Detail of Top URLs	23
Figure 15: Review dashboard	23
Figure 16: Request for review on email	23
Figure 17: Request for review on files	24
Figure 18: Policies & rules	24
Figure 19: Audit logs	25
Figure 20: Screenshot Microsoft Cloud Apps Discovery	25
Figure 21: Warning on share limitation of compromised file in OneDrive	31
Figure 22: Defender detected an e-mail with a malware-attachment	31
Figure 23: Defender alert details of EICAR detection	32
Figure 24: Alert timeline	32
Figure 25: Analysis	33
Figure 26: Example of alert about infrequent country (2020)	36
Figure 27: Detection of user at risk from Defender 365 Home dashboard	37
Figure 28: Overview of users at risk in the Azure admin portal	37
Figure 29: Risk detection details	38
Figure 30: Screenshots Microsoft "anonymization" option new reports and new	
sources in Cloud Discovery	40
Figure 31: Microsoft screenshot "anonymization" default in Cloud Discovery	41
Figure 32: Example of a request to measure.office.com	45
Figure 33: Example event Office.Taos.Shell.Impression.NavBarFull	46
Figure 34: Example event Office.Taos.Shell.Monitoring	47
Figure 35: Microsoft Twitter newsfeed embedded in the Admin Console	49
Figure 36: <u>Headers</u> traffic from Feedback form sent to office.com	50
Figure 37: Payload traffic from Feedback form sent to office.com	50
Figure 38: Reference to Privacy Policy in Microsoft Feedback form	50

Figure 39: Illustration provided by Microsoft for individual removal of Twitter fee	d 51
Figure 40: Microsoft detection types	56
Figure 41: Default retention period	60
Figure 42: Microsoft table of retention periods in Defender for Office 365	60
Figure 43 Export of Content Data from SharePoint, Exchange and Teams	63
Figure 44: Content export tool does not find Eicar test file in OneDrive	63
Figure 45: Microsoft explanation of the DSAR tool for diagnostic data	64
Figure 46: Microsoft commitment to provide Data Subject Access	64
Figure 47: Example of event related to use of Azure AD	70
Figure 48: Example of telemetry event with pseudonymised identifiers	71
Figure 49: Microsoft information about time to answer DSARs	71

#### Tables

10
43
45
45
65

### Summary

This report, commissioned by SLM Rijk, contains the results of a technical verification of Microsoft's data processing for security purposes through the use of Microsoft 365 Defender. This suite bundles different security services to protect devices, users, e-mail and login. The conclusions apply to both the Enterprise and the Education versions of Microsoft 365.

#### Nine verification questions

This report is based on nine verification questions.

- 1. Does Defender adequately detect critical threats and security breaches from devices and cloud apps, and with regard to malicious emails, files and URLs that are exchanged via e-mail and via OneDrive and Teams, both within the tenant and with external individuals?
- 2. Does Defender provide adequate warnings about suspicious logins via the Azure Active Directory?
- 3. How does the data anonymisation option work in Defender for Cloud Apps?
- 4. Does Microsoft send traffic to third parties (including through cookies, and to itself as an independent data controller) when a system administrator enables Defender? If so, are those third parties mentioned on the list of subprocessors?
- 5. Does Microsoft process learnings from security incidents across its Enterprise and Education user base, or are there limitations, such as prior anonymisation?
- 6. Does Defender create individual risk profiles and/or individual scores in the different analytic overviews and reports?
- 7. Does Microsoft publish adequate documentation on the personal data it collects through the tested applications, in comparison with captured network traffic and logs that are accessible for system administrators?
- 8. Does Microsoft give system administrators full access to all personal data it processes through the different Defender tools? Does Microsoft provide adequate explanations if it does not provide access to certain personal data?
- 9. Are there high risks resulting from the transfer of personal data to the USA or other third countries?

#### Outcomes

The main outcome of these tests is that Defender 365 does what it is supposed to do: inventory and protect devices, and detect malicious files, URLs, bulk mail and suspicious logins. Defender 365 does not recognise all possible malicious activity, for example old spyware, and gives the benefit of the doubt to 'known' sender domains. Following this logic, Defender assumes a high trust level for end users authenticated

with Microsoft's own Authenticator app. This makes Defender 365 less effective in determining the risks of 'known' and 'trusted' senders. This does not mean Defender is not capable of achieving the purposes for which it processes personal data: securing the work environment. The lack of alerts during some tests is a logical consequence of the limited test scope while Microsoft bases risk assessments on multiple criteria. These criteria could not all be replicated in the tests. For example: replicating a worldwide phishing campaign on multiple organisations was outside of the scope of the tests.

It follows from the tests that Microsoft does not automatically send personal data to external third parties, except for limited traffic to Twitter. Microsoft also qualifies itself as a third party (independent data controller) for the processing of personal and content data received through Feedback forms. It is not in line with the contractual privacy guarantees for Microsoft's Online Services that Microsoft decides itself when it is opportune to share any personal data with itself in a role as independent data controller, without any technical measure to centrally prevent this data flow.

#### **Reply and measures Microsoft April 2023**

Following a dialogue with SLM Rijk in April 2023, Microsoft clarified the purposes and scope of its data processing and transfers to the USA. Microsoft also improved its public documentation about the data processing for threat analysis. Though Microsoft previously used the words 'Insights' and 'Machine Learning', the use of these terms did not imply any personal data processing for global analytics. Microsoft clarified that it only transposes information about new threats to a list of known threats, without any customer information or personal data. Microsoft also acknowledged that device identifiers are personal data, and agreed to update its public documentation. Microsoft has committed to develop two options to block outgoing data traffic in the Defender admin console to Twitter and to centrally block the use of Feedback in Enterprise and Education tenants, or become a data processor for the Feedback data.

#### Remedies

In order to remedy the remaining issues with regard to the contractual privacy commitments, Microsoft and the government organisations / universities are advised to take the following remedies.

Question	Remedies Microsoft	Remedies organisations
Inventory and protect devices	No recommendations	Inform users about the data processing when they sign for receipt for their company-managed device.
Detect files, mails, apps and URLs	No recommendations	Avoid automatic deletion of suspicious mails.
		Allow employees to ask admins perform to perform a manual review on documents quarantined as malware.
		Allow the end user access to mails qualified as spam.

Detect suspicious logins	No recommendations	Instruct the admins to actively monitor for alerts on users at risk and to quickly follow up to make sure the detections are effective and the consequences of incorrect detections are minimised.
		Create a monitoring policy to restrict how admins are allowed to use the monitoring results, and inform the users about this personal data processing and the limits on its use.
		Consider using pseudonyms for employees whose identity should remain confidential
Data minimisation option Cloud Apps	Microsoft should use the term 'pseudonymisation' instead of 'anonymization'.	Use the pseudonymisation functionality to prevent unauthorised access to sensitive characteristics of end users that can be derived from their app usage.
		When using the temporary user data enrichment option to detect individual shadow IT usage, organisations must develop and communicate clear and knowable rules about the circumstances when these data can be accessed and for what specific purposes.
Traffic to third parties	Honour the two commitments to develop a setting to block the functionality of the <b>Twitter</b> feed and to offer a group policy or setting to centrally block the use of <b>Feedback</b> in Enterprise and Education tenants or become a data processor.	Use the central opt-out functionality for Twitter and Feedback.
Data reuse across userbase	No recommendations	No recommendations
Profiling	No recommendations	Provide a concise, intelligible and easily accessible internal explanation to employees about the data processing in Defender.

Docu- mentation	Microsoft must provide more information about the observed Telemetry Data from the admin portal, unless Microsoft is able to ensure that the browser telemetry data do not contain any identifying (pseudonymous) personal data.	No recommendations
Data Subject Access	Speed up the process of providing access.	No recommendations
	Stop collecting identifying data via the browser telemetry data or provide access to all personal data processed by Defender in a concise, transparent, intelligible and easily accessible form.	
	If Microsoft wants to rely on an exception to the access rights from Art. 23 (1) under i of the GDPR jo. Art. 41(1) sub i of the UAVG, Microsoft should explain the necessity in detail.	
Transfer risks	Complete the EU Data Boundary as soon as possible for all personal data, keep SLM Rijk up to date about the progress.	Accept the risks of transfer of pseudonymised server generate server logs and telemetry data to the USA until the end of 2023.
		Warn admins not to upload personal data in attachments with support tickets (transfer to the USA possible until the end of 2024).
		Consider using pseudonyms for specific employees working with secret data, and for system administrators.

### 1. Introduction

This report describes the results of a technical verification started in May 2022 of Microsoft's compliance with the privacy amendment negotiated in June 2019 by SLM Rijk (Strategic Vendor Management for Microsoft, Google and AWS) for specific online services that are part of Microsoft 365. In 2020, SURF, the Dutch umbrella ICT organisation for institutions of higher education, negotiated a similar privacy amendment. SLM Rijk commissioned Privacy Company to check Microsoft's compliance with the privacy guarantees for the online services for both Enterprise and Education version.

This report is a technical verification report. In reply to the findings of this report, Microsoft has provided clarifications and committed to develop data minimisation tools. As this technical verification report did not identify serious shortcomings, the results of this report will not be presented in a full DPIA report.

#### 1.1 Previous DPIAs on Microsoft Office 365

The cluster reports build on the (repeat) Data protection impact assessment (DPIA) on Office 365 for the Web and mobile Office apps published in July 2020.<sup>1</sup> The DPIA concentrated on the seven most frequently used Office applications, namely: Word, PowerPoint, Excel, Outlook, Teams, SharePoint and OneDrive, in combination with the Azure AD.

The DPIA concluded there were 6 high data protection risks for end-users of the software related to the processing of data about their use of the software and services (so-called Diagnostic Data). Between April and June 2020, SLM Microsoft Rijk and Microsoft agreed on measures to mitigate the six high data protection risks, as described in Section 17.3 of the DPIA. Some of the mitigating measures could be implemented fast, other mitigating measures required more time.

Privacy Company conducted a first check on the status quo of the implementation measures in August 2020, and found Microsoft complied with the 4 mitigating measures it had agreed to implement per 1 August 2020. In a second check, performed in April 2021, Privacy Company verified Microsoft's compliance with the remaining improvement measures, also with regard to some low risks found in the separate DPIA on Microsoft Intune.<sup>2</sup>

#### 1.2 Scope of this report: Microsoft 365 Defender

This report focusses on the data processing resulting from the use of Microsoft 365 Defender, hereinafter referred to as 'Defender'. This suite bundles different security services to protect devices, users, e-mail and login. Four services are in scope:

- 1. Microsoft Defender for Endpoint (MDE)
- 2. Microsoft Defender for Office 365
- 3. Microsoft Defender for Identity
- 4. Microsoft Defender for Cloud Apps3

- https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/06/30/dataprotection-impact-assessment-office-365-for-the-web-and-mobile-office-
- apps/DPIA+Office+for+the+Web+and+mobile+Office+apps+30+June+2020.pdf <sup>2</sup> Data protection impact assessment Intune, 30 June 2020, URL:
- https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/06/30/dataprotection-impact-assessment-intune/DPIA+Intune+30+June+2020.pdf

<sup>&</sup>lt;sup>1</sup> Data protection impact assessment Office 365 for the Web and mobile Office apps, 30 June 2020, URL:

<sup>&</sup>lt;sup>3</sup> Defender includes two other services that Privacy Company has not investigated, Defender for Cloud and Microsoft Sentinel. See: Microsoft Defender for Endpoint, 9 April 2023, URL: <u>https://learn.microsoft.com/en-gb/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=0365-worldwide</u>.

Figure 1:Illustration Microsoft tools in Microsoft 365 Defender<sup>4</sup>



Some Defender services had other names until 2022, namely Exchange Online Protection (EOP) and Office 365 Advanced Threat Protection (ATP). These features are now known as Defender for Office 365. The Defender for Cloud Apps service was previously called Microsoft Cloud Apps Security (MCAS). Only the name of Defender for Endpoint was unchanged.

The 15 most relevant Defender services for this DPIA are listed below in Table 1. Many of the services for Office and Identity can also be used to enrich reports on Endpoint and Cloud Apps; there is no longer a hard distinction between the four Defender services. The four services marked with an asterisk are not separately discussed in this report, as it involves the detection of individual malicious files or activities by system administrators. Hence the customer is in control of the scope of the data processing.

Defender	Service	Description and functionality
Endpoint	Device Inventory	Lists devices on the network, and whether they are
	Threat and	Dashboard showing potentially malicious files and device
	Vulnerability	behaviours
	Management	
Office and	Users at risk	List of potentially compromised users, both by behaviour
Identity		and logins from suspicious locations.
	Incidents &	Automatic alerts about cyber-attacks on the tenant or
	alerts	devices (in MDE)
	Threat analytics	New unknown viruses and malware in devices (MDE) and
		mailboxes
	Explorer	Suspicious emails, e.g. attachments with malware or
		content with phishing campaigns. Also includes tab "Top
		targeted users," the end users who most often receive
		such emails.
	Review	Overview of actions for system administrators, for
		example a manual review if a suspicious mail or file has
		been quarantined, or what to do with users blocked by

Table 1: Overview of relevant data processing services in Defender

<sup>&</sup>lt;sup>4</sup> Screenshot from Microsoft instruction video about Defender for Endpoint, URL: <u>https://www.microsoft.com/en-us/videoplayer/embed/RE4wDob?postJsllMsg=true</u>.

		Microsoft for sending too many messages classified as bulk mail.
	Policies & rules	Four sets of settings in Defender to help administrators manage threats: (i) Threat policies, (ii) Alert policies, (iii) Manage advanced alerts, and (iv) Activity alerts.
	Audit	Access to audit logs that Microsoft makes available to administrators.
	Hunting*	Specific security-related searches targeting users, devices (in MDE), specific alerts or configurations, e.g. look up user logins from specific countries, detect devices with outdated/vulnerable hardware, find malicious email attachments or malicious email senders.
	Actions & submissions*	Actions such as quarantining a malicious file, isolating a device, soft deletion of an email, initiating an antivirus scan or blocking URLs
	Exchange message trace*	Search the inboxes and logs of all end users in Exchange Online, for example, see all recent outgoing mail from a specific user after an incident. Or, check all incoming mail from a sender who sent malware once.
Cloud Apps	Cloud App Discovery dashboard and Cloud app catalogue	Cloud App Discovery dashboard and Cloud app catalogue Overview of used apps with security score and incidents.
	Activity Log*	Audit log of actions with apps such as login, file discard, search, attempted access by unauthorized app.
	Files	Overview of files flagged as malware, with information about the owner and the app in which the file was detected.

#### Out of scope

This report does not examine the processing of personal data through telemetry data from applications installed on end user devices, since this report focusses on the use of Microsoft's security cloud services. However, Section 5.2.2 does address the Telemetry Data collected by Microsoft from the browser of admins when they visit the Defender portal.

#### 1.3 Test methodology

This report is based on two separate inspections. In November 2020 Privacy Company assessed the data protection risks of some functionality of Cloud Apps and Defender for Endpoint for a government organisation, and processed the findings in a non-public report. In 2022 Privacy Company tested the data processing via the Defender for Office 365 tools for SLM Rijk, at the time known as Exchange Online Protection and Advanced Threat Protection, including Identity Protection through the Azure AD.

In 2020, the data processing was tested by performing scripted scenarios on workstations equipped with Windows 10 Enterprise by the government organisation that commissioned these first two reports. Two sets of test scenarios were performed on 5 November 2020. During the test scenarios a normal working day was simulated,

with opening and closing of documents and sending and receiving emails, etc. Selected malware was included in several ways to trigger responses by Defender for Endpoint. This lead to a large number of reported incidents. The generated data were sent to Microsoft's Defender cloud servers in Azure. When MDE discovered a possible security incident an investigation package was sent to the central service and was made available for inspection to the system administrators. The testing of Cloud Apps Security was limited to identity management and cloud apps discovery. The test scenarios included logging-in from an unusual country. Two data subject requests were subsequently filed with Microsoft to obtain any information it may have, that was not included in the available data in the audit logs and on the dashboard. Microsoft responded in December 2020 that it had not found any further information based on the identifiers provided by Privacy Company, only the given identifiers.

The inspections in 2022 were performed in a browser, as Defender for Office 365 is a cloud-based service. Privacy Company created a VM with a Dutch government's Enterprise license in a test tenant. The VM was equipped with Windows 10 Pro version 21H1, build no. 19043.1620 and the default browser Edge (version 100.0.1185.36). The browser versions of OneDrive, Teams and Outlook services were used to store and exchange files.

To answer the fourth question (about traffic to third parties), a dedicated test script was used with the Chrome browser 99.0.4844.84 and MiTM proxy version 6.0.2 to test for the existence of third-party traffic in the Admin console.

Tests were performed between 31 March 2022 and 1 April 2022. Microsoft's public documentation and information on the restricted access Admin Console was last reviewed in April and May 2023.

To minimise noise in the captured data traffic, the recommended privacy minimisation settings were followed in Office 365 (Additional Optional Connected Experiences disabled).

#### 1.4 About Microsoft 365 Defender

This report assesses the four major security tools included in Defender. These tools are briefly described in four paragraphs below. Essentially, Defender sends the information it collects about events to the Azure cloud servers dedicated to, and within the tenant of the customer. Microsoft also transfers some sample threat data to itself for advanced analysis, to be able to add newly discovered threats to the recognition patterns.

Microsoft describes the functionalities of Defender as follows:

"The **Microsoft 365 Defender portal** (<u>https://security.microsoft.com</u>) combines protection, detection, investigation, and response to email, collaboration, identity, device, and app threats, in a central place."<sup>5</sup>

<sup>&</sup>lt;sup>5</sup> Microsoft, Microsoft 365 Defender, 7 April 2022, URL: <u>https://docs.microsoft.com/en-</u> us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide

Figure 2: Microsoft graphic Core Defender services<sup>6</sup>



Figure 3: Microsoft illustration scale of Defender<sup>7</sup>

Scale and protection of Microsoft



The Defender portal provides access to 27 main sources of information. Microsoft is regularly adding new functionalities and tabs.

The current sources of information<sup>8</sup> are:

- 1. Incidents & alerts
- 2. Hunting
- 3. Actions & submissions
- 4. Threat analytics
- 5. Secure score (out of scope)
- 6. Learning hub (out of scope)
- 7. Trials (out of scope)
- 8. Device inventory
- 9. Vulnerability management (out of scope)

<sup>&</sup>lt;sup>6</sup> Screenshot taken from instruction video Microsoft about Defender for Endpoint, URL: <u>https://www.microsoft.com/en-us/videoplayer/embed/RE4wDob?postJsllMsg=true</u>

<sup>&</sup>lt;sup>7</sup> Microsoft, Machine learning and AI Innovation at Microsoft Security Research, URL: <u>https://www.microsoft.com/en-us/research/group/m365-defender-research/</u>. More details about the technical use of AI can be found in the blog, Improving AI-based defenses to disrupt human-operated ransomware, 21 June 2022, URL: <u>https://www.microsoft.com/en-</u> <u>us/security/blog/2022/06/21/improving-ai-based-defenses-to-disrupt-human-operated-</u> <u>ransomware/</u>

<sup>&</sup>lt;sup>8</sup> As checked on 1 May 2023 on security.microsoft.com.

- 10. Partners and APIs (out of scope)
- 11. Evaluation & tutorials (out of scope)
- 12. Configuration management (out of scope)
- 13. Investigations
- 14. Explorer
- 15. Review
- 16. Campaigns (not tested)
- 17. Threat tracker
- 18. Exchange message trace
- 19. Attack simulation training (out of scope)
- 20. Policies & rules
- 21. App governance
- 22. Reports
- 23. Audit
- 24. Health
- 25. Permissions and roles
- 26. Settings
- 27. More resources

#### Figure 4: Collated screenshots of Microsoft 365 Defender Homepage

Mercech 355 Defender	Sec. Sec.	and the second second	P lead	and the second second	•
tran		Home			
Endpoints .	~	Home			
Divice invention				Welcome to Micro	acoft 265
Vehicle in the second				welcome to witch	05011 303
Farthers and APA		0		Defender	
Evaluation & Seconds					
Configuration management		o		Inter Net step: Goe Section)	
Real & collaboration	1	0		Report to threats and manage security across	your identities, data, devices, apps, and
bradgetore .				attactucture, users more about the united exp	edence Coco-
buttown				Com	
heime				E Cuided tour	- 🖉 Whatsheet M Community + Ables
Campaigne					
Treat tracher					
Letterge message trace		Treat analytics -	Uses at this	Device compliance	Abus Sectorel Integration
Attack vimulation training		0 threats require	1 usans at sick	Interespecta compliance status	
Pations & rules		action	i users at risk		
Dout app	-	Emerging threat		Despiret Networgton	
Applychematics		A Exploration of the Logidy sub-enablity has been planned in multiple ango, fixed the report	State States for Hitsen		
		High-impact threats			
Reports .		Spring framment RCI universitätien 01	View all among	View details	
		00V-0537 colorizat actor targeting organisations 0/0			Unlock end-to-end
and the second second	100	for data sufficientian and destruction	Microsoft Secure Score -	Devices with active mahaare	visibility with Azure
multiplier to shares		Active allerta 📕 Basatived allerta 1 mare			Sentinel, your cloud-
maning		Highest exposure threats	Secure Score: 27.35%	No managed devices	native SIEM
Actions & submissions		Spring Frammunch BCE voluerabilities 0	Missional Secure Score is a representation of pour resentation's results excludes and exact security for	Tools security evens and ethora configuration and compliance parloas through intere device management	Connect Microsoft 393 Defender to Apure Sertinel to correcte finite-party data sources and per costolity across
Thread, analytics		DEV-40327 colorinal actor targeting organisations for 0 data sufficientian and destriation	mprova A	Taxante Tora, A. 1211	entry kill shares. Discoursed pricing for Microsoft 345 sustements is available.
Deriver lotten		and 21.53	125		
Learning hull:		Sex mane		Ensell devices	Enables Learn more
Train					1
Endpoints	a 20	ngawa k	11110000000000	Usars with threat detections	Security news feed
Device inventory			Monthly HLDTS	Users with thread detections.	
Volverability management	1		Appn 17.7%	Uni Alem	A feature of the destination
Partners and APts	14			Fast lana 1	Product terrs, security studigence, and trend resource.
Evaluation & Eclorada	~			1	
Configuration management					MSTICPy January 2012 harbathon toph
for all and the second second			Internet your score View Instance		reconcil and
town & construction	100		and the second sec		0 [*
investigations		Devices at risk -			Microsoft Security Intelligence a
Conner					The March 202 security unlates are available
Tarian .		0 device(s) at risk			https://witer.com/metaacompensari/orup/11212 400000215645813
Campagna		Device Risk level			1977 Fail
These tracker					· · · · · · · · · · · · · · · · · · ·
Exchange message trace					(Antheorem
Attack simulation training				-	Abstract continues in Averdar Howits Analysis
Policies & rules				Shere more	
Cloud apps			12000		100000000000000000000000000000000000000
			Simulation		Device health

#### 1.4.1 Defender for Identity

Defender for Identity uses information from the on-premises Active Directory to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions. $^9$ 

Defender for Identity offers two types of identity risk detection or calculation: Real-time and Offline.  $^{\rm 10}$ 

#### 1.4.2 Defender for Office 365

Defender for Office 365 protects against threats posed by email messages, links (URLs) and collaboration tools.

Defender for Office 365 includes *Exchange Online Protection (EOP)*, Microsoft's core email security tool. EOP checks all mails against blocklists for origin (spammers) and malware, and redirects all hyperlinks included in the body of e-mails to Microsoft, to be able to filter or trash malicious contents.

#### Microsoft explains:

"The message passes through content filtering (anti-spam and anti-spoofing) where harmful messages are identified as spam, high confidence spam, phishing, high confidence phishing, or bulk (anti-spam policies) or spoofing (spoof settings in anti-phishing policies."<sup>11</sup>



Figure 5: Microsoft illustration of EOP filtering<sup>12</sup>

<sup>&</sup>lt;sup>9</sup> Microsoft 365 Defender protection , URL: <u>https://learn.microsoft.com/en-us/microsoft-</u> <u>365/security/defender/microsoft-365-defender?view=0365-worldwide</u>

<sup>&</sup>lt;sup>10</sup> Microsoft, Risk types and detection, 16 February 2023, URL: <u>https://docs.microsoft.com/en-gb/azure/active-directory/identity-protection/concept-identity-protection-risks#risk-types-and-detection</u>.

<sup>&</sup>lt;sup>11</sup> Microsoft, Exchange Online Protection overview, 24 February 2023, URL:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/exchange-onlineprotection-overview?view=o365-worldwide

<sup>&</sup>lt;sup>12</sup> Idem.

Microsoft explains that Defender for Office 365 includes automated investigation and response capabilities.

"Microsoft Defender for Office 365 includes powerful automated investigation and response (AIR) capabilities that can save your security operations team time and effort. As alerts are triggered, it's up to your security operations team to review, prioritize, and respond to those alerts. Keeping up with the volume of incoming alerts can be overwhelming. Automating some of those tasks can help."<sup>13</sup>

#### Microsoft also explains it does not take automated remediation actions:

"In Microsoft Defender for Office 365, no remediation actions are taken automatically. Remediation actions are taken only upon approval by your organization's security team. AIR capabilities save your security operations team time by identifying remediation actions and providing the details needed to make an informed decision."<sup>14</sup>

#### 1.4.3 Defender for Endpoint

Defender for Endpoint monitors end-user devices running on multiple platforms (macOS, iOS, Linux, Android and Windows). Privacy Company has only done (limited) research on how Defender for Endpoint works, and only on Windows 10 devices. To protect the information on the device, MDE collects information about the processes active on the device, and scans incoming files and emails, trying to detect threats like viruses, hacking attempts and phishing. When MDE detects a potential threat, it will collect information about the event as well as of the state of the device at the time of the incident, including connection status, recent security events, domain names connected, and active and installed applications. To find potential threats, MDE scans emails and downloaded documents.

Microsoft explains how it sends feedback from detections both locally to the antivirus software on Windows 10 devices, and adds the newly discovered threat to the list of known threats:

"After incriminating an entity, Microsoft Defender for Endpoint stops the attack via feedback-loop blocking, which uses Microsoft Defender Antivirus to block the threat on endpoints in the organization. Defender for Endpoint then uses the threat intelligence gathered during the ransomware attack to protect other organizations."<sup>15</sup>

<sup>&</sup>lt;sup>13</sup> Microsoft, Automated investigation and response (AIR) in Microsoft Defender for Office 365, 28 February 2023, URL: <u>https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/air-about?view=o365-worldwide</u>.

<sup>&</sup>lt;sup>14</sup> Idem.

<sup>&</sup>lt;sup>15</sup> Microsoft, Improving AI-based defences to disrupt human-operated ransomware, 21 June 2022, URL: <u>https://www.microsoft.com/en-us/security/blog/2022/06/21/improving-ai-based-defenses-to-disrupt-human-operated-ransomware/</u>



#### Figure 6: Illustration Microsoft Defender for Endpoint<sup>16</sup>

To use the service, Microsoft Intune is required as device management software.<sup>17</sup> SLM Rijk has published a separate DPIA on Intune.<sup>18</sup> The data processing by Intune is outside of the scope of this report.

#### 1.4.4 Defender for Cloud Apps

Defender for Cloud Apps helps with security when working with cloud services. Defender for Cloud Apps acts as a gatekeeper, a *Cloud Access Security Broker*, to discover and provide visibility into Shadow IT and app use. It also monitors user activities for anomalous behaviours, controls access to the organisation's resources, can classify and prevent sensitive information breaches, protects against malicious actors, and helps to assess the compliance of cloud services.<sup>19</sup>

<sup>&</sup>lt;sup>16</sup> Idem.

<sup>&</sup>lt;sup>17</sup> Microsoft Defender portal, URL: <u>https://security.microsoft.com</u> .

<sup>&</sup>lt;sup>18</sup> SLM Rijk, Data protection impact assessment Intune, 30 June 2020, URL:

https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impactassessment-intune.

<sup>&</sup>lt;sup>19</sup> Microsoft Defender for Cloud Apps overview, 5 February 2023, URL:

https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps.



Figure 7: Microsoft illustration of Cloud Apps Architecture<sup>20</sup>

Depending on the configuration, Defender for Cloud Apps can route all traffic between the user and the selected cloud services through its system to scan all online traffic for potential malware (reverse proxy), collecting information from external cloud services through API-connectors and logs from the workstation.

Privacy Company has not tested this functionality but notes that such functionality would involve the processing of a wide array of personal data of the (external) data subjects whose data the government organisation is processing, as well as personal data relating to employees.

Microsoft explains: "Admins can search for a specific user's metadata or user's activity. Selecting an entity opens the Users page. The Users page provides you with comprehensive details about the entity that are pulled from connected cloud applications. It also provides the user's activity history and security alerts related to the user."<sup>21</sup>

#### 1.5 Different resources in Defender 365 portal

As Microsoft has merged the four different security tools in Defender, the results from the four tools are often presented in combined dashboards or reports.

<sup>&</sup>lt;sup>20</sup> Idem, under Architecture, URL: <u>https://learn.microsoft.com/en-us/defender-cloud-</u> apps/what-is-defender-for-cloud-apps#architecture.

<sup>&</sup>lt;sup>21</sup> Microsoft, Data security and privacy practices for Defender for Cloud Apps, 24 April 2023, URL: https://learn.microsoft.com/en-us/defender-cloud-apps/cas-compliance-trust.

Below, the 11 most relevant modules from the 16 modules mentioned in <u>Table 1</u> above are described to assess the risks of the data processing, with screenshots. This is followed by a summary list with a definition of the remaining accessible services for admins.

- 1. Device Inventory
- 2. Threat and Vulnerability Management
- Users at risk as shown in the Home portal (analysed separately in Section 3.2 of this report)
- 4. Incidents & alerts
- 5. Threat analytics
- 6. Explorer
- 7. Review
- 8. Policies & rules
- 9. Audit
- 10. Cloud App Discovery and Cloud app catalogue
- 11. Files

#### 1.5.1 Device Inventory

As shown in Figure 8 below, Defender shows overviews of connected devices and apps used by end users.

Figure 8: Screensl	not Microsoft	Device .	Inventory
--------------------	---------------	----------	-----------

ŵ	Home		De	evice Ir	nventory										
0	Incidents & alerts	$\sim$			Mahila Natura	t devices to T device									
0	Hunting	$\sim$	Co	mputers a	Mobile	k devices 101 device	5								
3	Actions & submissions	$\sim$		۸											
œ	Threat analytics			Cnbo	ard new devices	s are not protected									
Re	Learning hub														
			Tot	0.21	High risk	High exposure	iot onboarded								
12	Endpoints	^	12	.92K	10	14 1									
8	Device inventory		4	Export								0.50	wrh	30 Davs V III Customize o	columns 🔽 Filter
4	Vulnerability management	$\sim$	-									7 30	arch		
~d	Partners and APIs	$\sim$		Name		Domain	Risk level ⊙ ↓	Exposure level Ο	OS platform	Windows version	Sensor health state	Onboarding status	Last device update 🛈	Tags	Managed by 🛈
Ca	Evaluation & tutorials	$\sim$		ec2amaz-	hk672qp	Workgroup	High	A Medium	Windows Server 20		<ul> <li>Active</li> </ul>	Onboarded	Mar 2, 2022 1:29 PM	log4j	Unknown
	Foreit & collectored			adfs01.set	cxp.ninja	seccepininja	High	🔺 High	Windows Server 20		Active	Onboarded	Mar 2, 2022 11:24 AM	Device value: High	Unknown
	Email & consuboration			victimum.	na.contosohotels.com	na.contosohotels.com	High	A Medium	Windows Server 20		O Inactive	~ Onboarded	Feb 3, 2022 1:36 PM	log4j tester	Unknown
5	Emission			victim00.	na.contosohotels.con	na.contosohotels.com	High	A Medium	Windows Server 20		Inactive	Onboarded	Feb 4, 2022 3:43 AM	tester	Unknown
-7	Basisse			workstati	on16.seccxp.ninja	seccepuninja	High	A Medium	Windows 11	21142	Active	Onboarded	Mar 2, 2022 4:42 AM		Unknown
6	nevrew .			workstati	on6.seccxp.ninia	seccep.ninia	••• High	Low	Windows 10	21H1	• Active	< Onboarded	Mar 2, 2022 4 32 AM	HWA	MEM
0	Campaigns														
k2	Threat tracker			soc-fw-rd	p	Workgroup	Em Low	A Medium	Windows Server 20		<ul> <li>Active</li> </ul>	Onboarded	Mar 2, 2022 4:10 PM		Unknown
=	Policies & rules			shir-sap		Workgroup	Low	Low	Windows Server 20		O Inactive	< Onboarded	Feb 17, 2022 10:52 AM		Unknown

#### 1.5.2 Threat and Vulnerability Management

To detect vulnerable devices, the Microsoft Defender for Endpoint sensor automatically collects vulnerability and security data from the connected devices and publishes the results in the portal. It shows devices that were in use up to 30 days before.

#### Figure 9: Screenshot Microsoft Threat & Vulnerability Management dashboard<sup>22</sup>

≡ ŵ Home	Threat & Vulnerability Manage	ement dashboard		
Incidents & alerts ~				Filter by device groups (2/2)
₿ Hunting ~	Organization exposure score	Threat awareness ①		Microsoft Secure Score for Devices
Actions & submissions     Threat analytics	Exposure score	0 devices exposed to CVE-2021 The Logi vulnerability affects a Java logging component used in many soft	-44228	Your score for devices: 42%
Berdpoints     Device inventory	your organization Score is potentially impacted by active exceptions.	vulserable component might be exposed to remote code execution, which is Devices - onboarded Devices - not onboarded Vulne 0 0 0	an lead to full attacker control. able files Vulnerable software O	year devices acress OS, Application, Nehmark, Accounts and Security Controls Score is potentially impacted by active exceptions. 42(11)31 point actived Application \$/17
쇼 Vulnerability management ^		View vulnerability details		05 88/227 Network 55/103
Dashboard	12/100			Accounts 36/07
Recommendations	Low 0-29 Medium 30-69 High 70-100	Top security recommendations		Security controls 245/559
Software inventory	Exposure score over time	Recommendation E	posed devices Threats Impact Tags	
Weaknesses		Update Microsoft Windows Server 2016 (OS and built-in a., 31	s ∅ Õ ▼433	Score for devices over time
Event timeline	20	Update EDR sensor for down-level Windows Server 2	ilk @ (3 <b>▼</b> 245  +8.00	445
Evaluation & tutorials	0 02/13 02/23 02/27	Turn on Microsoft Defender for Endpoint sensor	Hik @ (3 ▼2.22  +7.19 COVID-19	42%. 42%. 02/06 02/13 02/20 02/27
Email & collaboration	Improve score	Show more Show exceptions		Improve score
C Investigations				
15 Explorer	Top events		Device exposure distribution	Top remediation activities
E Review	7 days		Exposure distribution	Remediation activities
Campaigns	Date (UTC) Event	Originally impocted devices (%)	Exposed devices are easy targets for cybersecurity attacks. Ensure	This table lists top activities that were generated from security
😰 Threat tracker	3/1/2022 II. Google Chrome has 21 new vulnerabilities, impacti	ng 65 devices 65 (2%)	that these devices can receive security updates, have critical security controls, and are properly configured.	Turn on real-time protection 10/14
车 Policies & rules	2/25/2022 🖳 Samba has 2 new vulnerabilities, impacting 1 device	1 (<1%)		Testin Testerin Testering
∠ Reports	2/28/2022 E. Samba has 2 new vulnerabilities, impacting 1 device	1 (<13)		Electronic reconcernation and a first contraction with a list

#### 1.5.3 Incidents & alerts

With *Incidents & alerts* Microsoft shows automatic warnings to an organisation about cyber-attack events detected by any tool in the Microsoft 365 Defender. The incidents can be prioritized by severity, and admins can identify affected end users by device and per mailbox. They can also investigate domains and URLs associated with a Microsoft Defender for Endpoint alert.

Figure	10:	Incid	ents	&	alerts

•	Alerts - Microsoft	365 security	× +	-							
÷	→ C	08=	https://security.microsoft.com/a	alerts				PCDPIATest tennant I	<b>₽</b> ☆	⊚ ± !	: =
	Microsoft 365 Defender	-	and the second second	P Search			K	-	-	⊚ ?	T
=											
ŵ	Home		Alerts								
Ø	Incidents & alerts	^	April 1st. Please refer to De	hat the MDE SIEM API is being dep precating the legacy SIEM API - Mi	recated on March 1st in a crosoft Tech Community fo	rost in Message cen r guidance on movir	iter (MC311064). For customers wh ing to alternative APIs and SIEM co	o are still using this API, we I mectors. If you need assistan	ave automatically ice in the migratio	extended the support until n, please contact support.	×
	Alerts		See the Microsoft 365 Com	pliance center for additional comp	liance-related functionality						×
6	Hunting Advanced hunting	^	$\pm$ Export 6 Months $\sim$	🖉 Manage alerts						Customize columns 🏾 🍸 Fi	ilter
	Custom detection rules		Alert name	Tags Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity	Last activ
3	Actions & submissions	^	eDiscovery search	III III III Informational	Queued	• New	Threat management	MDO	A Floor Terra	Apr 7, 2022 3:01 PM	Apr 7, 20
	Action center Submissions		eDiscovery search	間間間 Informational	Queued	New	Threat management	MDO	🛱 Floor Terra	Apr 7, 2022 2:57 PM	Apr 7, 20
6	Threat analytics		eDiscovery search	NIN Informational	Queued	New	Threat management	MDO	Roor Terra	Apr 7, 2022 2:56 PM	Apr 7, 20
₽	Secure score		eDiscovery search	### Informational	Queued	New	Threat management	MDO	A Floor Terra	Apr 7, 2022 2:55 PM	Apr 7, 20
%	Learning hub		eDiscovery search	### Informational	Queued	New	Threat management	MDO	A Floor Terra	Apr 7, 2022 11:33 AM	Apr 7, 20
咨	Trials		eDiscovery search	IIIII Informational	Queued	• New	Threat management	MDO	A Floor Terra	Apr 7, 2022 10:38 AM	Apr 7, 20
63	Endpoints	~	eDiscovery search	IN III III Informational	Queued	• New	Threat management	MDO	🖨 Floor Terra	Jan 25, 2022 11:16 AM	Jan 25, 2
	Device inventory		eDiscovery search	RIER informational	Queued	New	Threat management	MDO	Roor Terra	Nov 29, 2021 2:31 PM	Nov 29, 2
1	Vulnerability management	~	eDiscovery search	### Informational	Queued	• New	Threat management	MDO	🖓 Floor Terra	Nov 29, 2021 2:15 PM	0 9.7
٥đ	Partners and APIs	$\sim$									e
5	Evaluation & tutorials	~								ļ	
54	Configuration management										13

<sup>&</sup>lt;sup>22</sup> Screenshot from Microsoft instruction video Microsoft Defender for Endpoint, 7 February 2023, URL: <u>https://www.microsoft.com/en-us/videoplayer/embed/RE4wDob?postJsllMsg=true</u>.

Urls > dc2.domain1.te	st.local		Frame 631729			
ැ <sub>ව</sub> dc2.	domain1.te	st.local	/css/2110out.osa		+ Add indi	icator 🗠 View in explorer
Overview Incider Original URL dc2.domain1.test.loca URL summary Domain Details	I	<	Incidents & Alerts 39 active alerts, 14 incidents	Microsoft verdict Verdict: Phishing	Observed in Organization (Las 9 devices	t 30 Days) outrs 05/02
Domain Name dc2.domain1.test.loca View domain page	1		■ High (37)		Date (First / Last)	Devices
Registrant Domain Administrator	Registered on May 2, 1991 12:00 AM		New Inducing of Alerts		Apr 27, 2022 (Last)	□ cont-adrianbar
Updated on Apr 18, 2022 12:00 AM	Expires on May 3, 2023 12:00 AM					
Registrant Contact in	fo					
Country/Region						
Mailing address One Microsoft Way,, R	edmond, WA, US					

Figure 11: Screenshot Microsoft alert about suspicious domain<sup>23</sup>

#### 1.5.4 Threat analytics

*Threat analytics* is based on a set of reports from Microsoft security researchers. Microsoft describes that these reports cover the most relevant global threats, including:

- "Active threat actors and their campaigns
- Popular and new attack techniques
- Critical vulnerabilities
- Common attack surfaces
- Prevalent malware."<sup>24</sup>

The tool shows which of these global threats impact assets (devices or mailboxes). The admin can see devices with alerts, and devices with active and resolved alerts over time.<sup>25</sup>

Microsoft explains impacted mailboxes are "*mailboxes that have received email messages that have triggered Microsoft Defender for Office 365 alerts. While most messages that trigger alerts are typically blocked, user- or org-level policies can override filters.*"<sup>26</sup>

<u>365/security/defender-endpoint/investigate-domain?view=o365-worldwide</u>.

<sup>24</sup> Microsoft, Defender for Endpoint, Track and respond to emerging threats through threat analytics, 7 February 2023, URL: <u>https://docs.microsoft.com/en-us/microsoft-</u> <u>365/security/defender-endpoint/threat-analytics?view=o365-worldwide</u>.

<sup>&</sup>lt;sup>23</sup> Screenshot Microsoft, Investigate domains and URLs associated with a Microsoft Defender for Endpoint alert, 27 October 2022, URL: <u>https://learn.microsoft.com/en-us/microsoft-</u>

<sup>&</sup>lt;sup>25</sup> Idem.

<sup>&</sup>lt;sup>26</sup> Microsoft, Threat analytics in Microsoft 365 Defender, 8 March 2023, URL: <u>https://docs.microsoft.com/en-us/microsoft-365/security/defender/threat-analytics?view=0365-worldwide</u>

In the test tenant, as shown in <u>Figure 12</u> below, this did not lead to any alerts, because the tests were performed with known, old malicious files and this tool only shows alerts for the current most important global threats.

Figure 12: (Global) threat analytics

Threat analytics -	- Microsoft 360	× +							
- → C	08=	https://security.m	icrosoft.com/tl	hreatanalytics3			PCI	OPIATest tennant 🛍 😫 🏠	© ± #
Microsoft 365 Defender		and the second		P Sea	rch			the second	
Home		Threat a	inalytic	s					
Incidents & alerts	^	Ransomware	Phishing	Vulnerability	Activity group				F
Incidents		37	12	61	49				Email notification settings
Alerts									
Hunting	^	Latest threats				High-impact threats O		Highest exposure threats	
Advanced hunting		CVE-2022-2327	B: Microsoft D	efender for Endpo	oint 0/0	Simulated threat	0/0		
Custom detection rules		spoofing vulner	ability			WannaCrypt	0/0		
Actions & submissions	^	BlackCat ranson	nware		0/0	BadRabbit	0/0		
Action center		Spring Framewo	ork RCE vulner	rabilities	0/0	Smoke Loader (Dofoil) mines coin	0/0		
Submissions		DEV-0537 crimi data exfiltration	nal actor targe n and destruct	eting organization ion	s for 0/0			High 70-100	a law 0.29
Threat analytics						Mo slarte Recolud slarte Active slarte		a right to-too a meanin so-a	0000-23
Secure score		🖩 No alerts 📕 R	esolved alerts	Active alerts		In the alerts Preserved alerts Active alerts			
Learning hub		O Search				1	-30 < > 022	Choose columns 🗸 📋 30 items	per page 🖂 🍸 Filters
Trials		Threat				Alerts	Impacted ass	ets   Threat exposure level	Misconfigured devices
Endpoints	~	CVE-2022-232	78: Microsoft D	Defender for Endpo	int spoofing vuln	rability 0 active /	二 0	Not available	Not available
Device inventory		BlackCat ranso	smware			0 active /	D0	Not available	Not available
Vulnerability management	~	Spring Framev	vork RCE vulner	rabilities		0 active /	<u>_</u> 0	Not available	Not available
Partners and APIs	~	DEV-0537 crim	ninal actor targe	eting organizations	for data exfiltrat	on and destruction 0 active /		Not available	Not available
Evaluation & tutorials	~	OSX/Shlayer s	ustains adware	push		0 active /	O	Not available	Not available

### 1.5.5 Explorer

The tool *Explorer* discloses Microsoft's detection of suspicious emails, for example, attachments with malware, or content with phishing campaigns. One of the tabs discloses the 'Top targeted users', in other words, the end users that most frequently receive such mails. It is also possible to view the 'Top URLs', with an indication what Microsoft has done with the URL. Each URL shown in that list provides a hyperlink to the specific end users that have visited those URLs.

Microsoft is able to collect this information about visited URLs because Exchange Online Protection has an in-build URL replacement that redirects all clicks to Microsoft itself, in order to detect and possible junk or quarantine malicious files. See <u>Figure 5</u> in Section 1.4.2 of this report.





Figure 14 below illustrates details of the Top URLs in the Explorer dashboard.

#### Figure 14: Detail of Top URLs

			Chart time zone: (UTC +02:00)	
告	Vulnerability management	$\sim$	Delivered Delivered to junk Eliocked	
۰đ	Partners and APIs	$\sim$	Email URL clicks Top URLs Top clicks Top targeted users Email origin Campaign	
C2	Evaluation & tutorials	$\sim$		
5	Configuration management		UR.	Messa
	Email & collaboration	^		
Ģ	Investigations		docs.microsoft.com/microsoft-sos/compliance/collection-statistics-reports	-
5	Explorer		www.rustica.fr/nl/2932/u/7Nh8gnONj9i1Lczazcho1%2Bl8wabqEldIRCk8fprwH3tAkxHQ5O5kl%2FKG62wWmIga28uLaMyuGcmc1dyIUQMZgYyKt2BZMYH7ij3j9zhSPg%3D/siteurl	
	Review		www.rustica.fr/data/img/newsletter/2022-03-10/api-images-cover-160xnull-622715f3660f4e003beece2b-bf838632844c48ec9321e48eca630191.png	
0	Campaigns		www.findasianbeauty.com/e/07/c2.jpg	
¥	Threat tracker		docs.microsoft.com/microsoftteams/teams-powershell-supported-versions	
0:	Exchange message trace		www.rustica.fr/data/img/newsletter/2022-03-10/api-images-cover-160xnull-622715f3660f4e003beece2b-cfa91e67370b815a23ac97ca104782b7.png	
围	Attack simulation training		www.findasianladies.com/images/logo.png	
=	Policies & rules		d15k2d11r6t6rLcloudfront.net/public/users/Integrators/BeeProAgency/685926_668466/ER%20Capital/afm-banner-lg.jpeg	1

#### 1.5.6 Review

As illustrated in Figure 15 below, with the dashboard *Review* system administrators get an overview of actions to take. If Microsoft has quarantined a suspicious mail or file, it asks the administrator for a 'review', that is, what the administrator wants to do with the mail or file. Another review task is to decide what to do with users that have been blocked by Microsoft for sending too many messages classified as bulk mail. See Figure 16 below.

#### Figure 15: Review dashboard

• •	Review - Microsoft	365 security ×	+								
÷	→ C	O A ## htt	tps://security.microsoft.com/three	streview			PCDPIATest tennant	# # ☆	0	*	 =
	Microsoft 365 Defender			P Search			and the				FT)
•3	Partners and APIs Connected applications API explorer Partner applications	ŕ	Review Action Center		Quarantine		Restricted Users				
	Professional services Evaluation & tutorials Evaluation lab Tutorials & simulations Configuration management	^	Track phish malware ca aimed at ye and take ag action.	ing and mpaigns sur users spropriate	Revi mes whe relev mor recip	ew quarantined sages and decide ther you want to se them to one or of the intended ients.	P.	nblock users who ave been blocked for ending too many vessages marked as pam/bulk.			
	Email & collaboration	^									
	Explorer Review		Malware trends								

#### Figure 16: Request for review on email

	Microsoft 365 Defender	De lette	and the second		P Search						© ?
-											
ŵ	Home		Review >	Quarantine							Ca Learn more
Ø	Incidents & alerts	~									
6	Hunting	~	Email	Files							
9	Actions & submissions	$\sim$	These messi decide whet	ages were quarantined ther you want to releas	because they were classified a e them to one or more of the i	s malware, spam, phishing, or bulk, i ntended recipients. Learn more abov	or because of a ma ut quarantined ema	il flow rule (transp iil messages	ort rule) in your orga	nization. Review the	messages and
G	Threat analytics		C) Refrest	h / Release / A	pprove release 🕞 Deny 📋	Delete messages 🛭 😂 Preview m	essage ···· More	~	1 item 🔎 Sea	rch	7 5 = √
8	Secure score		Filters: Tin	ne received: Last 30 da	ys.						
R,	Learning hub		Time	a received	Subject	Sender	Quarantine reason	Release status	Policy type	Expires	Recipient
10	Trials				ander	Service -			, ./pt		
			Apr	4, 2022 4:51:06 PM	Eicar test	Floor@PCdpiaTest	Malware	Needs review	Anti-malware policy	Apr 19, 2022 2:00:0	floor.terra@privacy
40	Endpoints	~									

Figure 17: Request for review on files

iii Microsoft 365 Defende		P se	irch		1		
101							
බ Home		Review > Quarantine					🞑 Learn more
① Incidents & alerts	~						
🕞 Hunting	~	Email Files					
Actions & submissions	~	These messages were quarantined because they decide whether you want to release them to one	were classified as malware, spam, or more of the intended recipient	phishing, or bulk, or because of a mail flow rule (trans s. Learn more about guarantined email messages	port rule) in your orga	nization. Review th	e messages and
Threat analytics		C) Refresh		3 items 0 Searc		Filter 😨 Custor	nize columns 🛛 = 🗸
Secure score		Filters: Time received: Last 30 days Quaranti	ne reason: Malware 🗙				
Re Learning hub		User	Location	Attachment filename	File URL	Release status	Expires
ලී Trials		Floor@PCdpiaTest.onmicrosoft.com	OneDrive	4c1dc737915d76b7ce579abddaba74ead6fdb5b	https://pcdpiatest-my.	Needs review	Apr 19, 2022 2:00:0
Eð Endpoints	~	Floor@PCdpiaTest.onmicrosoft.com	OneDrive	smb-gab_1g0l.bin	https://pcdpiatest-my.	Needs review	Apr 19, 2022 2:00:0
Device inventory		Floor@PCdpiaTest.onmicrosoft.com	OneDrive	eicar.com	https://pcdpiatest-my.	Needs review	Apr 19, 2022 2:00:0

#### 1.5.7 Policies & rules

With *Policies & rules* Microsoft offers four sets of settings in Defender to help admins manage threats: (i) Threat policies, (ii) Alert policy, (iii) Manage advanced alerts and (iv) Activity alerts.

With (i) Threat policies the admin decides how strict for example DKIM controls are set, or what the threshold for the number of received mails to qualify such mail as bulk mail. The admin also decides when the end user is notified if mail is qualified as spam and if mail is quarantined. By default, the option to notify senders is disabled. If enabled, the organisation risks to alert malware senders that their behaviour is detected.

With the (ii) Alert Policy the admin decides how high the threat must be before an alert is sent, in many different threat categories.

The other two options are out of scope of this report.

		Delicies & ndes	Mensel 10	* +		
4	→ C	- restances	08=	* https://security.microsoft.com/securitypoliciesandrules	PCDPIATest ternant 💼 🚼 🟠	☺ ± ∷ ≡
	Micros	oft 365 Defende		P. Search	1 de ma	○ ? (7)
유. 전	Learning Trials	hub		Policies & rules		
13	Endpoint	s:	~	Set up policies to manage devices, protect against threats, and receive alerts about various activities in you	ur organization. Learn more	
	Device in	ventory				4 items
4	Vulnerabi	lity management	$\sim$	Name		
۰đ	Partners a	ind APIs	~	Threat policies		
73	Evaluation	8 tutorials	~	Alert policy		
57	Configura	tion management		Manage advanced alerts		
	Email & c	ollaboration	^	Activity alerts		
φ,	Investigat	ions				
5	Explorer					
E	Review					
0	Campaigr	15				
k2	Threat tra	cker				
0:	Exchange	message trace				
<u>B</u>	Attack sin	ulation training				0
当	Policies 8	rules				
٥	Cloud ap	ps	~			

Figure 18: Policies & rules

#### 1.5.8 Audit

*Audit* provides access to the service generated server logs made available by Microsoft as audit logs. See <u>Figure 19</u> below.

#### Figure 19: Audit logs<sup>27</sup>

Export 🗸						23
Date ↓	IP Address	User	Activity	Item	Detail	
Apr 1, 2022 3:41 PM	45.137.101.242	Floor@PCdpiaTest.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed	
Apr 1, 2022 3:40 PM	45.137.101.242	Floor@PCdpiaTest.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed	
Apr 1, 2022 3:40 PM	45.137.101.242	Floor@PCdpiaTest.onmicrosoft.com	User logged in	00000003-0000-0000-c000-00000000		
Apr 1, 2022 3:40 PM	45.137.101.242	Floor@PCdpiaTest.onmicrosoft.com	User logged in	00000003-0000-0000-c000-00000000		
Apr 1, 2022 3:40 PM	45.137.101.242	Floor@PCdpiaTest.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed	
Apr 1, 2022 3:40 PM	45.137.101.242	Floor@PCdpiaTest.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed	
Apr 1, 2022 3:40 PM	45.137.101.242	Floor@PCdpiaTest.onmicrosoft.com	User logged in	00000002-0000-0ff1-ce00-000000000		
Apr 1, 2022 3:39 PM	45.137.101.242	Floor@PCdpiaTest.onmicrosoft.com	UserLoginFailed	00000002-0000-0ff1-ce00-000000000		
Apr 1, 2022 3:35 PM		NOT-FOUND	SearchMtpStatus			
Apr 1, 2022 1:35 PM		NOT-FOUND	SearchMtpStatus			
Apr 1, 2022 11:35 AM		NOT-FOUND	SearchMtpStatus			
Apr 1, 2022 9:35 AM		NOT-FOUND	SearchDataInsightsSubscription			
Apr 1, 2022 9:35 AM		NOT-FOUND	SearchTIKustoClusterInformation			
Apr 1, 2022 9:35 AM		NOT-FOUND	SearchMtpStatus			
Apr 1, 2022 7:35 AM		NOT-FOUND	SearchMtpStatus			
Apr 1, 2022 5:35 AM		NOT-FOUND	SearchMtpStatus			
	Export × Date ↓ Apr 1, 2022 3:41 PM Apr 1, 2022 3:40 PM Apr 1, 2022 3:39 PM Apr 1, 2022 3:39 PM Apr 1, 2022 1:35 PM Apr 1, 2022 1:35 PM Apr 1, 2022 1:35 AM Apr 1, 2022 9:35 AM Apr 1, 2022 9:35 AM Apr 1, 2022 9:35 AM Apr 1, 2022 9:35 AM	Export         IP Address           Apr 1, 2022 3:41 PM         45.137.101.242           Apr 1, 2022 3:40 PM         45.137.101.242           Apr 1, 2022 3:30 PM         45.137.101.242           Apr 1, 2022 3:35 PM         45.137.101.242           Apr 1, 2022 3:35 PM         45.137.101.242           Apr 1, 2022 1:35 AM         45.137.101.242           Apr 1, 2022 3:35 PM         45.137.101.242           Apr 1, 2022 3:35 PM         45.137.101.242           Apr 1, 2022 3:35 AM         45.137.101.242           Apr 1, 2022 9:35	Export ~           Date 1         IP Address         User           Apr 1, 2022 3:41 PM         45137.101.242         Roor@PCdpiaTest.onmicrosoft.com           Apr 1, 2022 3:40 PM         45137.101.242         Roor@PCdpiaTest.onmicrosoft.com           Apr 1, 2022 3:30 PM         45137.101.242         Roor@PCdpiaTest.onmicrosoft.com           Apr 1, 2022 3:35 PM         NOT-FOUND         NOT-FOUND           Apr 1, 2022 1:35 PM         NOT-FOUND         NOT-FOUND           Apr 1, 2022 1:35 PM         NOT-FOUND         Apr 1, 2022 9:35 AM         NOT-FOUND           Apr 1, 2022 9:35 AM         NOT-FOUND         Apr 1, 2022 9:35 AM         NOT-FOUND           Apr 1, 2022 9:35 AM         NOT-FOUND         Apr 1, 2022 9:35 AM         NOT-FOUND	Export ×           pate 1         P Address         User         Activity           Apr 1, 2022 3:41 PM         45.137.101.242         Floor@PCdpiaTestonnicrosoft.com         Accessed malibox items           Apr 1, 2022 3:40 PM         45.137.101.242         Floor@PCdpiaTestonnicrosoft.com         Accessed malibox items           Apr 1, 2022 3:40 PM         45.137.101.242         Floor@PCdpiaTestonnicrosoft.com         User logged in           Apr 1, 2022 3:40 PM         45.137.101.242         Floor@PCdpiaTestonnicrosoft.com         User logged in           Apr 1, 2022 3:40 PM         45.137.101.242         Floor@PCdpiaTestonnicrosoft.com         Accessed malibox items           Apr 1, 2022 3:40 PM         45.137.101.242         Floor@PCdpiaTestonnicrosoft.com         Accessed malibox items           Apr 1, 2022 3:30 PM         45.137.101.242         Floor@PCdpiaTestonnicrosoft.com         User logged in           Apr 1, 2022 3:35 PM         45.137.101.242         Floor@PCdpiaTestonnicrosoft.com         User logged in           Apr 1, 2022 3:35 PM         VIT.FOUND         SearchMtpStatus           Apr 1, 2022 1:35 PM         NOT-FOUND         SearchMtpStatus           Apr 1, 2022 9:35 AM         NOT-FOUND         SearchMtpStatus           Apr 1, 2022 9:35 AM         NOT-FOUND         SearchMtpStatus           Apr 1, 2022	Bappert V     Inter I PAddress User VIIII VIIII PAddress User VIIII VIIII VIIII VIIII VIIIII VIIIII VIIIII VIIIII VIIIIII	Eport         PAders         Der         Aciny         Izen         Detal           Ap1, 2022 34 PM         5137.0124         Foorl@Cpialetomicrostros         Cessed mailor items         Mailones         Mailetens           Ap1, 2022 340 PM         5137.0124         Foorl@Cpialetomicrostros         Cessed mailor items         Conconconcentros         Mailetens           Ap1, 2022 340 PM         5137.0124         Foorl@Cpialetomicrostros         Cessed mailor items         Conconconcentros         Mailetens           Ap1, 2022 340 PM         5137.0124         Foorl@Cpialetomicrostros         Cessed mailor items         Conconconcentros         Mailetenscentros           Ap1, 2022 340 PM         5137.0124         Foorl@Cpialetomicrostros         Cessed mailor items         Mailetenscentros         Mailetenscentros           Ap1, 2022 340 PM         5137.0124         Foorl@Cpialetomicrostros         Cessed mailor items         Mailetenscentros         Mailetenscentros           Ap1, 2022 340 PM         5137.0124         Foorl@Cpialetomicrostros         Cessed mailor items         Soccentros         Mailetenscentros           Ap1, 2022 340 PM         5137.0124         Foorl@Cpialetomicrostros         Cessed mailor items         Soccentros         Soccentros         Soccentros         Soccentros         Soccentros         Soccentros         Soccent

#### 1.5.9 Cloud App Discovery dashboard and Cloud app catalogue

As shown in <u>Figure 20</u> below, the Cloud Discovery dashboard has different tabs, including information about discovered apps that may be shadow ICT, and behaviour per user and per device.

::: Microsoft 365 Defender			> Search		_				
≡		Cloud Discovery							
D Insidents & alaste		cioud Discovery					Win10 Endpoint Users	s ∨ () Last 30 days ∨ Ac	ions 🗸 🔞
<ul> <li>Incidents or alerts</li> </ul>		Updated on Sep 27, 2022, 4:09 PM							
C> Hunting	Ň	Dashboard Discovered apps Discovered re	esources IP addresses Users Devices						
Actions & submissions	~								
(1) Threat analytics		Acos IP addresses	Users Devices	Traffic		Cloud Discovery open alerts		+ (	Treate policy
Secure score		20 2	1 2	1200	Ŧ 552 MB	2.0			
Re Learning hub		20 2		1.5 GB	₹ 814 MB	38 Goud Discovery	alerts 🖬	<ul> <li>Suspicious use alerts</li> </ul>	
沿 Trials									
*     Ø Partner catalog	~	App categories		<1-5 of 35 F Traffic	- EB	Risk levels	All categories	✓ by Traffic	v 83
Assets	^		🖾 🛚 Sanci	tioned 🛛 🖬 Unsanctioned	🖬 🕻 Other				
9. Identities		Coud storage			713 M8		Traffic from bi	ah risk anns	
		Collaboration			409 M8	1.3 GB	Traffic from m	edium risk apps	
Email & collaboration	^	Security			164 MB	Total	Traffic from low	w risk apps	
C Investigations		Content management			36 MB		O Configure so	ore metric	
5 Explorer									
E Review									
③ Campaigns		Discovered apps	<1-15 of 20 + View all apps All categories	♥ Traffic	v 🖽	Top entities	View all users User	✓ by Traffic	v 🖪
😒 Threat tracker				Sanctioned Unsanctioned	Other	User			Total
1 Attack simulation training				• on an country	242.442	Second and a second second			13.08
若 Policies & rules		<ul> <li>Dropook</li> <li>Slack</li> </ul>			399 MB	Jawiliuca-restation			1.5 GB
		O CloudFlare			79 MB				
Cloud apps	^	<ul> <li>Akamai</li> </ul>			62 MB				
68 Cloud discovery		Could discovery Cogle			27 MB				
H Cloud app o		Microsoft Teams			20 M8				
8º OAuth apps		DigiCert			14 M8	Apps headquarters location		All categories	
App governance		Microsoft Bing			9 MB		8 de 1	à	Ģ
-		0 000			0 140			1	

Figure 20: Screenshot Microsoft Cloud Apps Discovery<sup>28</sup>

 $<sup>^{\</sup>mbox{\tiny 27}}$  Screenshot made in the government test tenant on 1 April 2022.

<sup>&</sup>lt;sup>28</sup> Screenshot from Microsoft 365 Defender instruction video, URL: <u>https://www.microsoft.com/en-</u>

gb/videoplayer/embed/RE59yVU?postJsllMsg=true&autoCaptions=en-gb

#### 1.5.10 Activity Log

The Activity log allows admins to search for specific activities with policies, for example a search for activities performed on certain files. Microsoft explains: "you can use the Activity log to find users in your organization who are using operating systems or browsers that are out of date, as follows: After you connect an app to Defender for Cloud Apps in the Activity log page, use the advanced filter and select User agent tag. Then select Outdated browser or Outdated operating system."<sup>29</sup>

#### 1.5.11 Files

With Files, organisations can scan all files for modifications, for example all the files stored in OneDrive and Salesforce. The modification can be to content, metadata, or sharing permissions. Organisations can also use the Files functionality to investigate what kind of data are saved in cloud apps.<sup>30</sup>

#### 1.5.12 Description of other resources in Defender 365

Organizations may choose to install **Antivirus (Next Generation Protection)** on Windows devices. The service uses information from multiple sensors in the operating system as well as machine learning, big data analytics and threat research to protect devices. This is out of scope of this report.

The resource **Hunting** enables admins to perform specific security related queries based on the security logging collected by the four different tools in Defender. This tool uses Kusto Query Language, that enables quick hunting over tons of records. The queries can be aimed at users, devices, specific alerts or configurations, to help organisations find and investigate security incidents.

Examples of use cases are:

- Look-up user logins from specific countries. This can be useful to investigate if hackers from a specific country such as China have attempted to log in after one account is compromised by a hacker from that country;
- Find all devices with outdated vulnerable hardware that needs to be upgraded;
- Find malicious email attachments;
- Find malicious senders of mail.

The resource **Actions & submissions** enables organisations to take actions such as quarantining a malicious file, isolating a device, soft deleting an email, starting an antivirus scan or blocking URLs.

**Secure score** provides essential security organisations to organisations based on existing Microsoft security tooling. This is similar to the Compliance score in the Microsoft 365 compliance center, with a slightly different scope. This is out of scope of this report.

<sup>&</sup>lt;sup>29</sup> Microsoft Defender for Cloud Apps, Activities, 24 April 2023, URL:

https://learn.microsoft.com/en-us/defender-cloud-apps/activity-filters. <sup>30</sup> File filters in Microsoft Defender for Cloud Apps, 5 March 2023, URL: https://learn.microsoft.com/en-us/defender-cloud-apps/file-filters.

**Reports** offers different reports and dashboards of data that are also disclosed via other tabs, such as the homepage (with the view of *Users at risk*) and email & collaboration reports (a category that for example contains the Explorer results).

The *Learning hub* offers links to articles, videos, blogs and interactive training.

The resource **(Threat)** *Investigations* enables organisations to create scripts to automatically log investigations and start responding to the logged security incidents.

The module *Campaigns* provides warnings about phishing and malware attacks, as identified and categorised on the customer tenant. The test tenant was not subjected to such campaigns during the (brief) testing period, and therefore, this module was not tested.

**Threat tracker** provides information about cybersecurity issues via different widgets. For example: there is a wave of Russian attacks on Ukrainian sources, show if specific employees are at risk.<sup>31</sup> This module could not be tested in the test tenant, due to the limited testing time and limited test employees.

**Exchange message trace** provides a hyperlink to the Exchange Online Environment. An admin can use this tool to search for the inboxes and logs of all end users. When an incident has occurred related to a specific end user, the admin may for example want to inspect all recent outgoing mails of that user. Or, if the organisation receives malware from a specific sender, the admin may want to check all incoming mail from that sender.

**Trials** offers access to 90 day free trials of different Defender tools, but this is out of scope of this targeted verification report.

The module **Health** contains two items: Service health and Message Center. *Service Health* provides information about interruptions of Microsoft services and incident advisories. *Message Center* contains a wide variety of update messages from Microsoft, for example related to Office, Windows or Defender feature updates.

**Permissions & roles** enables admins to view the permissions within the organisation for access to Defender.

**Settings** shows some privacy relevant settings generally determined in other tools, such as the geolocation of data and the chosen data retention periods. Settings offers some choices such as enabling feature preview or adding specific mail addresses for alerts.

**More resources** offers hyperlinks to other Microsoft security tools, such as Azure AD Identity Protection and Azure Information Protection. The resources **App governance**, **Device inventory**, **Vulnerability management**, **Partners and APIs**, **Evaluation & tutorials**, **Device configuration management** and **Attack** 

<sup>&</sup>lt;sup>31</sup> Microsoft, What are threat trackers?, 6 April 2022, URL: <u>https://docs.microsoft.com/en-gb/microsoft-365/security/office-365-security/threat-trackers?view=o365-worldwide#what-are-threat-trackers</u>.

*simulation training* are out of scope of this report, as they relate to either device management, Cloud App security or to trainings.

### 2. Verification questions

This report is based on the following nine verification questions:

- 1. Does Defender adequately detect critical threats and security breaches from devices and cloud apps, and with regard to malicious emails, files and URLs that are exchanged via e-mail and via OneDrive and Teams, both within the tenant and with external individuals?
- 2. Does Defender provide adequate warnings about suspicious logins via the Azure Active Directory?
- 3. How does the data anonymization option work in Defender for Cloud Apps?
- 4. Does Microsoft send traffic to third parties (including through cookies, and to itself as an independent data controller) when a system administrator enables Defender? If so, are those third parties mentioned on the list of subprocessors?
- 5. Does Microsoft process learnings from security incidents across its Enterprise and Education user base, or are there limitations, such as prior anonymisation?
- 6. Does Defender create individual risk profiles and/or individual scores in the different analytic overviews and reports?
- 7. Does Microsoft publish adequate documentation on the personal data it collects through the tested applications, in comparison with captured network traffic and logs that are accessible for system administrators?
- 8. Does Microsoft give system administrators full access to all personal data it processes through the different Defender tools? Does Microsoft provide adequate explanations if it does not provide access to certain personal data?
- 9. Are there high risks resulting from the transfer of personal data to the USA or other third countries?

The questions are answered by a short description of the relevant facts, such as available settings, public information or improvement commitments from Microsoft.

Per question, the section with the facts is followed by a description of the relevant technical findings, an assessment of the legal consequences of the technical findings and suggestions for mitigating measures.

### 3. Detection of malicious files, apps and URLs

This section answers the first verification question:

Does Defender adequately detect critical threats and security breaches from devices and cloud apps, and with regard to malicious emails, files and URLs that are

exchanged via e-mail and via OneDrive and Teams, both within the tenant and with external individuals??

#### 3.1 Facts

As data processor for Office and/or Microsoft 365 Enterprise (for Education), Microsoft must assist the data controllers (the Dutch government organisations and universities) with their security posture. Based on Art. 28 of the GDPR (processor obligations) this includes (in abbreviated descriptions):

- taking all measures required pursuant to Article 32 [security measures] (Art. 28 (3) sub c);
- assisting the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 [compliance with security and DPIA obligations] (Art. 28 (3) sub f);

In order for data controllers to demonstrate that Microsoft complies with its processor obligations, the government and university admins must be able to verify the effectivity of the security tools, to establish that the data processing is necessary to comply with GDPR and specific government security obligations.

#### 3.2 Technical findings

As described in the Section 1.3 of the Introduction, Privacy Company performed tests on two of the tools in November 2020 (Defender for Endpoint and Cloud Apps Security), and on the two other tools in April 2022 (Defender for Identity and Defender for Office 365).

For all tools, a limited test was performed with known malware to reduce the risk of triggering an actual malware incident. Both in 2020 and 2022 Privacy Company performed several tests with the EICAR<sup>32</sup> anti-malware test file.

In 2020 Privacy Company tested Defender for Endpoint (on the Windows device) with other examples of tools that can be used for data exfiltration: Mimikatz software to steal login credentials from a Windows PC (in 2020), FileZilla and Tor. Privacy Company also tested the data processing via Cloud Apps Security by downloading a diabetes app.

In 2022 Privacy Company downloaded *Bonzi Buddy* (a famously aggressive adware program disguised as freeware desktop virtual assistant, launched in 2000 and terminated in 2004<sup>33</sup>) in the OneDrive, as well as a sample of the WannaCry-malware. The WannaCry sample was not shared outside of the test tenant to reduce the risk of an actual incident.

Privacy Company performed the tests as follows:

• Use of the laptop to (attempt to) download en send the EICAR test virus via the installed Outlook app.

<sup>&</sup>lt;sup>32</sup> <u>https://www.eicar.org/?page\_id=3950</u>

<sup>&</sup>lt;sup>33</sup> <u>https://en.wikipedia.org/wiki/BonziBuddy</u>

- Attempt to download Mimikatz on the Windows 10 device
- Install the MedM Diabetes app from the Windows Store on the Windows 10 device.
- Use of Outlook for the Web and Teams for the Web on a Windows 10 device; sending and receiving files within the tenant and with external users.
- Use of OneDrive for the Web on a Windows 10 device; uploading and downloading files and sharing the files.

The result in 2020 was that Defender for Endpoint detected, and prevented the downloading of EICAR and Mimikatz. The Diabetes app was downloaded to check what data Cloud Apps Security collected about the name/nature of the app in its logfiles. The outcome was that Defender for Endpoint does not structurally log all network traffic and installed apps on a device, only in case of security incidents.

When MDE detects a possible security incident, it creates an "*investigation package*", that contains information about the state of the device at the time of the incident. This investigation package is sent to the Defender cloud service in Azure and available for inspection to the system administrators. Microsoft can also use this information for its own advanced analysis.

The investigation package contains a lot of information about the end user device, including all installed applications, current network connections (including local and internet connections and DNS requests) and running processes (what software is active on the device). The logs in the package all contain references to device and user identifiers. Most of these logs contain very technical information that is not very revealing of the user, but some of these may be quite sensitive. The DNS cache in particular may contain information about the political, religious, or arguably sexual interests of the data subject derived from web surfing or app usage on the device.

The results in 2022 were that Defender for Office 365 and Defender for Identity showed several alerts, as shown in Figures 21

<u>Figure 22</u> below. However, no limitations were observed on the sharing of *Bonzi Buddy* (the ad/spyware program).



Figure 21: Warning on share limitation of compromised file in OneDrive

Figure 22: Defender detected an e-mail with a malware-attachment

-

←→ ♂ 00	H #2 https://security.microsoft.com/threatexplorer	PCDPIATest tennant IIII 📲 😭	⊚ 坐 🗉
iii Microsoft 365 Defender	P Serch	the -	◎ ?
Tutorials & simulations	Sender ✓     Use commas (.) to separate multiple entries. Click Refresh to filter the results.       ♥ Advanced filter     2022-03-14       □     0000       •     -       2022-04-12     □       2359     •	Refresh	Save query $\vee$
Email & collaboration	Malware family $\sim$		≟ Export chart data
C Explorer	13		
E Review	g 1		
Campaigns	as as		
🖄 Threat tracker			
Exchange message trace	0 Apr A, 2022 230 AM		
🖪 Attack simulation training	Chart time zone: (UTC + 023	20)	
🟥 Policies & rules	Email Top malware families Top targeted users Email origin Campaign		~
○ Cloud apps ^	Message actions $$	1 item 🚽 Export email list	Customize columns
App governance	Date (UTC +02:00) Subject Recipient T	lags Sender Additional act	Latest deliver Original deliv
🗠 Reports	Apr 4, 2022 4:51 PM Elcar test 🖾 floor terra@privacycompany.nl -	Floor@PCdpiaTest.onmi	Quarantine Quarantine
🖹 Audit			

This resource enables admins to take a deep dive in the nature and origin of files marked as suspicious. As shown in Figures <u>23, 24 and 25</u> below, Microsoft shows the most important event metadata, such as affected user, type of action taken, type of incident and timestamp, with underlying information about all the details.

Figure 23: Defender alert details of EICAR detection

Tags	$\sim$
Detection details	^
Threat	
Malware ,Spam	
Latest delivery location	
Quarantine	
Original delivery location	
Quarantine	
Detection technology	
General filter, Antimalware protection	
Delivery action	
Blocked	
No overrides	$\sim$
Email details	^
Directionality	
Outbound	
Recipient (To)	
floor.terra@privacycompany.nl 🗅	
Sender (From)	-
Floor Terra <floor@pcdpiatest.onmicr< td=""><td>Ю</td></floor@pcdpiatest.onmicr<>	Ю
Time received	
4 Apr 2022 16:51	
Internet Message ID	L.
<pa4p190mb1263200f27bfda9270f4< td=""><td>Ю</td></pa4p190mb1263200f27bfda9270f4<>	Ю
Network Message ID	
22072co0_0d00_48a1_1426_08da164a8	Ð
55575CE5-0005-40a1-1420-060a104a6	
Cluster ID	

#### Figure 24: Alert timeline

Timeline Analy	vsis Attach	iments URL	Similar emails			
⊥ Export 🖒 Re	fresh			1 item	✓ Search	Customize columns
Timeline	Source	Event types	Result	Threats	Details	
4 Apr 2022 16:51	System	Original delivery	Quarantine - Blocked	Malware,Spar	m Detection technol	logy: Antimalware protection, Gener
# Figure 25: Analysis

Timeline Analysis Attachments URL Similar emails				
Email detection details				
System override(s) ① None		Exchange Transport Rule(s) 💿 7de4a805-4197-4584-bc56-fb9b0963334b 🗅		
		Go to Exchange Admin Center		
Junk mailbox rule 🔘		Bulk complaint level (BCL) 💮		
Spam confidence level (SCL) 🕥		Policy		
Policy action		Client type		
		OWA		
Sender-Recipient details				
Sender name		Sender IP		
Floor Terra		2a10:3781:412:1:38aa:8257:2d3b:c0d0		
Domain name		Domain owner		
Location		Domain creation date		
		14 Apr 2022 💿		
Return-path		P2 sender		
Floor@PCdpiaTest.onmicrosoft.com		Floor@PCdpiaTest.onmicrosoft.com		
То		Ce		
Floor Terra <floor.terra@privacycompany.nl></floor.terra@privacycompany.nl>				
Forwarding				
Authentication				
Domain-based Message Authentication (DMARC)		DomainKeys identified mail (DKIM) ①		
None		None		
Sender Policy Framework (SPF) ③		Composite authentication ③		
Related entities				
Entity	Total count		Threats found	
Attachments	1		Yes	
URLs	0		No	

#### 3.3 Assessment

Organisations need an adequate protection layer to protect the personal data they process on the devices, in Office and in the Active Directory. Absent adequate protection there would be imminent risks to the rights and freedoms of employees, as well as of clients and contacts of the government organisation and to the continuity and integrity of the operations of the government organisation itself.

The main outcome of these tests is that Defender 365 does what it is supposed to do: detect malicious files, apps and URLs. However, this verification report is not a security assessment. The effectiveness against relevant threats needs to be assessed by each individual organisation implementing Defender 365.

The spyware *Bonzi Buddy* was included in the test to assess detection of a class of software that is not necessarily classified as malware. It is highly unlikely that an organisation would want their employees to install *Bonzi Buddy* on their work-computers. Since this spyware was not detected, Defender 365 would not be the recommended solution against this category of risks.

For spam containing malicious URL's protection is similarly present but not absolute. E-mails containing malicious links are blocked, however some slipped through without detection. This is probably due to the fact that Microsoft takes the account properties of the sender into account, and not only the contents. In the test set-up malicious mails and spam were forwarded from existing Microsoft e-mail accounts (live.com). This possibly lead to a lower risk score. Some of these bulk mails were blocked, but not all. It appears that Defender 365 gives the benefit of the doubt to 'known' sender domains. This makes Defender 365 less effective in determining the risks of 'known' senders.

This does not mean Defender is not capable of achieving the purposes for which it processes personal data: securing the work environment. The lack of alerts during some tests is a logical consequence of the limited test scope while Microsoft bases risk assessments on multiple criteria. These criteria could not all be replicated in the tests. For example: replicating a worldwide phishing campaign on multiple organisations was outside of the scope of the tests.

The tests show that end users receive clear information when files and e-mails are blocked. By default, they can access mails qualified as spam in a separate spam box. Malicious files that are put in quarantine can be reviewed by the admin. The admin can perform a manual check of the file before the file is permanently deleted, or automatically reject malicious files. By default quarantined files are kept in quarantine for 15 or 30 days, depending on the reason for the quarantine. They are deleted after that period. Microsoft explains that admins can change the retention period for messages quarantined by anti-spam policies (including spam, high confidence spam, phishing, high confidence phishing or bulk) and for messages quarantined by anti-phishing policies (including spoof intelligence in EOP; user impersonation, domain impersonation, or mailbox intelligence in Defender for Office 365).<sup>34</sup>

The sender of the suspicious files and mails on the other hand does not receive feedback from Microsoft that mail was blocked or quarantined. This default setting makes perfect sense, because if Microsoft were to send feedback, malicious senders could learn from the feedback to try to bypass the filters.

### 3.4 Remedies

The first assessment <u>does not lead to recommendations to Microsoft</u>. However, this first analysis <u>does lead to three recommendations to the system administrators</u> responsible for the settings in Defender.

- 1. Avoid automatic deletion of suspicious mails
- 2. Allow employees to ask admins perform to perform a manual review on documents quarantined as malware
- 3. Allow the end user access to mails qualified as spam

Automated deletion of spam mails is a type of automated decision making that can significantly affect the data subjects sending (legitimate) e-mails. For example, if they apply for a job but their application is deleted, or if there is a legal requirement to send a document before a fixed date, but the mail allegedly is never received.

<sup>&</sup>lt;sup>34</sup> Microsoft, Quarantined email messages in EOP and Defender for Office 365, 18 March 2022, URL: <u>https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages?view=0365-worldwide</u>.

# 4. Detection of suspicious logins in the Azure AD

This section answers the second verification question:

Does Defender provide adequate warnings about suspicious logins via the Azure Active Directory?

# 4.1 Facts

Defender includes detection of the following categories of risky login types.

- Activity from anonymous IP address
- Anomalous token
- Anonymous IP address
- Atypical travel
- Azure AD threat intelligence
- Impossible travel
- Malicious IP address
- Malware linked IP address
- Mass access to sensitive files
- Nation state IP
- New country
- Password spray
- Possible attempt to access Primary Refresh Token (PRT)
- Suspicious browser
- Suspicious inbox forwarding
- Suspicious inbox manipulation rules
- Suspicious sending patterns
- Token issuer anomaly
- Unfamiliar sign-in properties

Microsoft explains in a whitepaper about Azure Active Directory Data Security Considerations: "*Azure AD Identity Protection uses real-time user login data along with multiple signals from company and industry sources to feed to its*  *machine learning systems to detect anomalous logins.* Personal data is scrubbed from this real-time login data before it is passed into the machine learning system, along with the remaining login data used to identify users and logins that are potentially risky."<sup>35</sup>

# 4.2 Technical findings

In 2020 the MCAS functionality was tested to warn about suspicious logins, based on Azure AD Identity Protection. For the purpose of the test, logins were made from unusual foreign countries by signing in from a collection of Tor-exit nodes. MCAS correctly identified the infrequent country and generated an alert (in this case: Morocco).



Figure 26: Example of alert about infrequent country (2020)

In 2022 Privacy Company performed tests simulating 'suspicious' logins by signing in from a collection of Tor-exit nodes using an account secured by the Microsoft Authenticator app. <u>None of the logins was marked as suspicious</u>.

Re-testing <u>without the Microsoft Authenticator app</u>, but with SMS as second factor did yield an alert of one user at risk. In order to simulate a login attempt on a user account from multiple locations that cannot physically be reached in that short a time span, the test account was used to log in from Tor-exit nodes from Russia, Germany, Brazil and from a consumer IP in the Netherlands. Defender detected this behaviour and labelled this attack as a 'password spray' attack.

<sup>&</sup>lt;sup>35</sup> Microsoft whitepaper, Azure Active Directory Data Security Considerations, 1 July 2020, URL: <u>https://azure.microsoft.com/en-us/resources/azure-active-directory-data-security-considerations/</u>.



Figure 27: Detection of user at risk from Defender 365 Home dashboard

Clicking through this alert takes the administrator to the Azure admin portal showing the detected risks.

Figure 28: Overview of users at risk in the Azure admin portal

Floor Terra - Ris	k detections 👒 –							×
🕕 Learn more 🛓 Down	oad 🔘 Refresh 🕴 🎫 Columns	R Got feedback?						
Auto refresh : Off User detections Workk	Detection time : Last 1 month	Show dates as : Local Us	ser starts with b2814ab7-0cdb-4b7c-98fe-26deea	388bb3 Detection type : N	ione Selected	Risk state : 2 selected	Risk level : None Selected	Add filters
Detection time †.;	User †	IP address ?↓	Location	Detection type $ \hat{\tau}_{\psi} $	Risk state 斗		Risk level 14	Request ID 11
4/1/2022, 10:52:01 AM	Floor Terra	185.220.100.242	Hassfurt, Bayern, DE	Password spray	At risk		High	46414223-5673-4a74-a936-065847 ***
3/30/2022, 10:51:36 AM	Floor Terra	45.12.134.107	Amsterdam, Noord-Holland, NL	Password spray	At risk		High	dec4e06c-a8ec-4d79-96af-c81c2e7 ···

Selecting the risk detection details reveals that Microsoft labelled the logins as a 'Password spray', that is, repeated attempts to log in to the user account. This classification is likely made because password sprays are often done through a large collection of different hosts rather than through a single host.

Figure 29: Risk detection details

# **Risk Detection Details**

攭 User's risk report	t Ͽ User's sign-ins 🛛 Ə User's risky sign-ins 🖤
Detection type P	assword spray 🕕
Risk state A	.t risk
Risk level H	ligh
Risk detail -	
Source lo	dentity Protection
Detection timing C	Offline
Activity	Sign-in
Detection time	4/1/2022, 10:52 AM
Detection last update	ed 4/1/2022, 2:43 PM
Token issuer type	Azure AD
Sign-in time	3/31/2022, 5:20 PM
IP address	185.220.100.242
Sign-in location	Hassfurt, Bayern, DE
Sign-in client	Mozilla/5.0 (Windows NT 10.0; rv:91.0)
Sign-in request id	4f414223-5673-4a74-a936-065847895700
Sign-in correlation ic	bb4dd8fc-efa5-4c9a-b5f0-0176a7e9717f

Defender 365 allows the admin to export the list of detected risky logins as a CSV or JSON file with the following output (transposed by Privacy Company for readability).

Table ET Example of	
Request ID	e1029815492d27508f7f8f7f6eee5aaf be568ad289d4647ebdbb4ff2616c8111
Correlation ID	bb4dd8fc-efa5-4c9a-b5f0-0176a7e9717f
Detection type	Password spray
Risk state	At risk
Risk level	High
Risk detail	-
Source	IdentityProtection
Detection timing	Offline
Activity	Sign-in

Table 2: Example of exported risky logins

Activity time	44651,7226
Detection time	44652,4528
Detection last updated	44652,6133
User object ID	b2814ab7-0cdb-4b7c-98fe-26deea388bb3
User	Floor Terra
UPN	Floor@PCdpiaTest.onmicrosoft.com
IP address	185.220.100.242
Location	Hassfurt - Bayern - DE
Detection time Detection last updated User object ID User UPN IP address Location	44652,4528 44652,6133 b2814ab7-0cdb-4b7c-98fe-26deea388bb3 Floor Terra Floor@PCdpiaTest.onmicrosoft.com 185.220.100.242 Hassfurt - Bayern - DE

# 4.3 Assessment

Defender does provide alerts about suspicious logins, but did not generate alerts about logins from multiple countries (through Tor exit nodes) from an end user authenticated with the Authenticator app. Apparently, Microsoft raises the trust level of a login attempt when the user is authenticated through Microsoft's own app.

When the logins from the Tor exit nodes were authenticated with SMS as second factor, Defender signalled the user was at risk.

Based on these limited tests, the service functions as expected.

In order to adequately protect the tenant against malicious logins, admins need to finetune Defender and actively monitor its alerts. Unlike Defender's ability to block files containing malware user risk detections do not necessarily lead to blocked behaviour. For certain risky behaviour types, like logging in from certain countries, admins need to take additional measures. When a user is at risk the admin needs to investigate the alert. Defender can be configured to pro-actively alert admins or specific people depending on the type and severity of the detected risks.

When user risk detections are used in conjunction with additional measures like multi-factor authentication and active monitoring by admins to follow up on alerts, this feature of Defender can be an effective security measure.

#### 4.4 Remedies

This assessment does not lead to a recommendation for Microsoft, but <u>organisations</u> can take three measures to reduce possible data protection risks.

- 1. Instruct the admins to actively monitor for alerts on users at risk and to quickly follow up to make sure the detections are effective and the consequences of incorrect detections are minimised.
- 2. Create a monitoring policy to restrict how admins are allowed to use the monitoring results, and inform the users about this personal data processing and the limits on its use.
- 3. Consider using pseudonyms for employees whose identity should remain confidential.

# 5. Data minimisation options

This section answers the third question:

How does the data anonymization option work in Defender for Cloud Apps??

# 5.1 Facts

Microsoft offers an pseudonymisation option for user names in the dashboards from Defender for Cloud Apps. If used, username information is replaced with encrypted usernames. Microsoft calls this "*data anonymization*", but also points out the admins can resolve the real username if necessary for a specific security investigation. Such lookups/conversions are logged in the Governance log. This log allows organisations to check if admins have correctly reidentified, in line with the internal privacy policy.<sup>36</sup>

Microsoft describes three ways to use this option: for new snapshot reports or reports from new data sources (see <u>Figure 30</u> below) or by setting the default to anonymisation under Cloud Discovery.

Figure 30: Screenshots Microsoft	"anonymization"	option	new	reports	and	new
sources in Cloud Discovery <sup>37</sup>						

Create new Cloud Discovery snapshot report	Add data source
O VURNEW O VURNEW O NAPPICE LODS  Report Name *  Description  Source *  Select applance.  V	Name * Comment Source * Select appliance  Receiver type * Select receiver type  Comment
Anonymize private information     Store and display only encrypted user names     C Protocol     Road 3	Generate web traffic logs for this data source  Anonymize private information Store and display only encrypted usernames. Add

<sup>&</sup>lt;sup>36</sup> Microsoft, Cloud Discovery data anonymization, 24 April 2023, URL: <u>https://learn.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-anonymizer</u>, and Data security and privacy practices for Defender for Cloud Apps, 24 April 2023, URL: <u>https://learn.microsoft.com/en-us/defender-cloud-apps/cas-compliance-trust</u> <sup>37</sup> Microsoft, Cloud Discovery data anonymication

 $<sup>^{\</sup>rm 37}$  Microsoft, Cloud Discovery data anonymization



Figure 31: Microsoft screenshot "anonymization" default in Cloud Discovery<sup>38</sup>

By default Microsoft does not include the identifiable user names in its cloud discovery logs. Admins can choose to include the Azure Active Directory username data in the Cloud Discovery data. This would have the opposite effect from the anonymisation option, and include the names in the logs processed by Microsoft.

Microsoft explains enabling this feature can be useful for the detection of shadow IT:

- "You can investigate Shadow IT usage by Azure Active Directory user. The user will be shown with its UPN.
- You can correlate the Discovered cloud app use with the API collected activities.
- You can then create custom logs based on Azure AD user groups. For example, a Shadow IT report for a specific Marketing department."

### 5.2 Assessment

Privacy Company has <u>not tested</u> these two anonymisation and identification options, but noted in 2020 that this process of hiding the user names falls under the Art. 4 (5) GDPR definition of pseudonymisation. Because the process is reversible (by the admins and by Microsoft) use of this option does not result in anonymous data. The resulting data set are still personal data, because the definition of personal data includes all data that can be directly or indirectly related to a natural person.

With regard to the directly identifying names in the 'enriched' Cloud Discovery logs, Microsoft explains in its Azure AD Whitepaper from 2020 that it does not use directly identifying data in logs for its own purposes. "Usage data is metadata generated by the Azure AD service that indicates how the service is being used. This metadata is used to generate administrator and user facing reports and is also used by the Azure AD engineering team to evaluate system usage and identify opportunities to improve the service. This data is generally written to log files, but in some cases, is

<sup>&</sup>lt;sup>38</sup> Idem.

collected directly by our service monitoring and reporting systems. personal data is stripped out of Microsoft's usage data prior to the data leaving the originating environment."<sup>39</sup>

Microsoft uses the term anonymization too loosely, not in compliance with the GDPR. However, use of this pseudonymisation tool can prevent high data protection risks. Through the use of apps, end users may reveal health data, religious, political or sexual characteristics. Hiding the user names prevents admins from immediate identification of these users. Microsoft has also created audit logs that will register any attempt to reidentify the data. This is a good technical measure to ensure such reidentification is only done when justified.

If organisations want to identify specific users to detect shadow IT usage, they must ensure that access to, and use of these potentially sensitive data is strictly necessary for legitimate purposes. As this information can potentially be used in evaluation reports to negatively assess individual employees, organisations must meet a high threshold for transparency and purpose limitation.

### 5.3 Remedies

• Microsoft should use the term 'pseudonymisation' instead of 'anonymization'.

Organisations can take two mitigating measures:

- 1. Use the pseudonymisation functionality to prevent unauthorised access to sensitive characteristics of end users, derived from their app usage.
- 2. Prior to using the user data enrichment option, organisations must have clear and knowable rules about the circumstances when these data can be accessed and for what specific purposes. Organisations must likely involve their Workers Council when updating their internal privacy policy with these rules.

# 6. Traffic to third parties

This section answers the fourth verification question:

Does Microsoft send traffic to third parties (including through cookies, and to itself as an independent data controller) when a system administrator enables Defender? If so, are those third parties mentioned on the list of subprocessors?

# 6.1 Facts

As data processor, Microsoft may only engage authorised subprocessors to process the personal data from Dutch government organisations and universities (art 28 (3) sub d, which refers to the obligations in Art. 28 (2) and Art. 28 (4) of the GDPR.

Microsoft publishes a limitative list of subprocessors for the Online Services in its overview of Data Protection Resources, last changed on 23 November 2021.<sup>40</sup> The

 <sup>&</sup>lt;sup>39</sup> Microsoft whitepaper, Azure Active Directory Data Security Considerations, 1 July 2020.
 <sup>40</sup> Microsoft Online Services Subprocessor List, Last updated 23 November 2021.

https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downlo adType=Document&downloadId=926b2cf5-6b6e-43ca-9bc3-f73e961aad5f&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913 Subprocessor List

most relevant change compared to the July 2020 version is the removal of the US American company *UserVoice* (specialised in digital customer research) as a subprocessor to process customer questions about the Microsoft services.<sup>41</sup> In 2021 Microsoft started to use its own (1<sup>st</sup> party) user discussion forums.<sup>42</sup>

# 6.2 Technical findings

Privacy Company intercepted and recorded outgoing traffic from the test VM while the Admin Console was accessed with a Chrome browser. This resulted in HTTP(S) requests to the domains listed in <u>Table 3</u> below.

Requests to domains highlighted in <u>green</u> are the result of Chrome browser functionality and not the result of using any Defender services and are therefore out of scope. The domains highlighted in <u>yellow</u> are explained in more detail below the table. This includes traffic to 2 Microsoft telemetry domains, traffic to 4 Microsoft analytics domains and traffic to 6 Twitter (sub)domains.

The intercepted traffic is analysed below in four categories. Necessary functional traffic to Microsoft is not separately analysed. There is a difference between telemetry traffic to known telemetry network domains from Microsoft, and traffic related to website analytics, even though such analytics are collected from the browser in a similar way as the telemetry data. Next to these two categories, traffic to Twitter and traffic to other third parties is discussed below.

Domain	No. of requests
accounts.google.com	1
clients1.google.com	1
clients2.google.com	1
sb-ssl.google.com	1
www.google.com	20
clientservices.googleapis.com	1
content-autofill.googleapis.com	14
optimizationguide-pa.googleapis.com	2
safebrowsing.googleapis.com	3
update.googleapis.com	19
www.googleapis.com	4
clients2.googleusercontent.com	7
lh5.googleusercontent.com	2
encrypted-tbn0.gstatic.com	6
www.gstatic.com	1

Table 3: Traffic from the Defender Admin Console

https://slmmicrosoftrijk.nl/?smd process download=1&download id=3485.

<sup>&</sup>lt;sup>41</sup> Microsoft's use of UserVoice was described in the June 2020 DPIA on Office for the Web and mobile Office apps for SLM Rijk, p. 48-49, URL:

<sup>&</sup>lt;sup>42</sup> Microsoft, UserVoice pages, URL: <u>https://support.microsoft.com/en-us/office/uservoice-pages-430e1a78-e016-472a-a10f-dc2a3df3450a</u>.

edgedl.me.gvt1.com	19
login.live.com	1
waconafd.officeapps.live.com	4
waconatm.officeapps.live.com	2
admin.microsoft.com	37
browser.pipe.aria.microsoft.com	<mark>14</mark>
browser.events.data.microsoft.com	4
graph.microsoft.com	3
security.microsoft.com	218
login.microsoftonline.com	21
arc.msn.com	3
prod.msocdn.com	3
ecs.office.com	1
741fda1a90fc5da8166f072f2a86ddd8.fp.measure.office.com	2
8f475c157813105fc1b2e28e76fbb96a.fp.measure.office.com	2
config.fp.measure.office.com	1
upload.fp.measure.office.com	2
portal.office.com	22
webshell.suite.office.com	4
ow1.res.office365.com	2
r4.res.office365.com	1
static2.sharepointonline.com	3
abs.twimg.com	3
pbs.twimg.com	24
cdn.syndication.twimg.com	6
ton.twimg.com	2
platform.twitter.com	11
syndication.twitter.com	8
dc.services.visualstudio.com	52
spoprod-a.akamaihd.net	14
scc.azureedge.net	146
aadcdn.msauth.net	20
amcdn.msftauth.net	1
res.cdn.office.net	24
res-1.cdn.office.net	13
admincontrolsdemoapps.blob.core.windows.net	1

# 6.2.1 Traffic to Microsoft analytical (sub)domains

Requests to the subdomains at *measure.office.com* appear to collect analytical information about the use of the Compliance Centre. These requests do not contain cookies, but the requests do contain the pseudonymous identifier of the tenant, as highlighted in yellow in <u>Figure 32</u> below.

Figure 32: Example of a request to measure.office.com

https://upload.fp.measure.office.com/r.gif?MonitorID=O365se&rid=c0fec6277f1366fec6f5dafb ab30748f&w3c=true&prot=https:&v=20190214&tag=[{"TenantId":"bd9a989d-e990-4e6e-9566-5a8b29c3b6ff","AppId":"ComplianceCenter"} ]&DATA=[{"RequestID":"8f475c157813105fc1b2e28e76fbb96a","Object":"trans.gif","Conn":"c old","Result":663,"T":128,"Rip":"2a10:3781:412::","Ep":"MDW","Fe":"cafe"},{"RequestID":"8f 475c157813105fc1b2e28e76fbb96a","Object":"trans.gif","Conn":"warm","Result":215,"T":128, "Rip":"2a10:3781:412::","Ep":"MDW","Fe":"cafe"},{"RequestID":"waconafd.officeapps.live.co m","Object":"trans.gif","Conn":"cold","Result":140,"T":128,"Ep":"PIE1","Fe":"WordLB1"},{"Re questID":"waconafd.officeapps.live.com","Object":"trans.gif","Conn":"warm","Result":130,"T": 128,"Ep":"PNL1","Fe":"WordLB1"},{"RequestID":"waconatm.officeapps.live.com","Object":"trans.gif","Conn":"cold","Result":84,"T":128,"Ep":"PNL1","Fe":"WordLB1"},{"RequestID":"waconatm.officeapps.live.com","Object":"trans.gif","Conn":"cold","Result":84,"T":128,"Ep":"PNL1","Fe":"WordLB1"},{"RequestID":"waconatm.officeapps.live.com","Object":"trans.gif","Conn":"cold","Result":84,"T":128,"Ep":"PNL1","Fe":"WordLB1"},{"RequestID":"waconatm.officeapps.live.com","Object":"trans.gif","Conn":"cold","Result":84,"T":128,"Ep":"PNL1","Fe":"WordLB1"},{"RequestID":"waconatm.officeapps.live.com","Object":"trans.gif","Conn":"cold","Result":84,"T":128,"Ep":"PNL1","Fe":"WordLB1"},{"RequestID":"waconatm.officeapps.live.com","Object":"trans.gif","Conn":"cold","Result":84,"T":128,"Ep":"PNL1","Fe":"WordLB1"},{"RequestID":"waconatm.officeapps.live.com","Object":"trans.gif","Conn":"Cold","Result":18,"T":128,"Ep":"PNL1","Fe":"WordLB1"}]

As shown in <u>Table 4</u> below, the full request headers do not contain any cookies.

sec-ch-ua	" Not A;Brand";v="99", "Chromium";v="99", "Google Chrome";v="9
	9"
sec-ch-ua-mobile	?0
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.
	36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
sec-ch-ua-platform	"macOS"
accept	*/*
origin	https://security.microsoft.com
sec-fetch-site	cross-site
sec-fetch-mode	cors
sec-fetch-dest	empty
referer	https://security.microsoft.com/
accept-encoding	gzip, deflate, br
accept-language	en-GB,en-US;q=0.9,en;q=0.8

Table 4: Full request headers to measure.office.com (r	(no cookies)
--	--------------

#### 6.2.2 Telemetry data sent to Microsoft

Privacy Company observed Telemetry Data being transmitted to two different domains while using the admin portal: browser.pipe.aria.microsoft.com and browser.events.aria.microsoft.com.

Table 5: Telemetry events transmitted to Microsoft

Event names	Number
Office.Taos.Shell.Impression.NavBarFull	2
Office.Taos.Shell.Monitoring	6
Office.Taos.Shell.Performance	2
Office.Taos.Shell.ServerRequest	4
awt_stats	3

generic_qos	2
impression	2
monitoring	6
performance	2
prefetch_request	2
searchbox_performance	2
serverrequest	4
session	4

The contents of two of these events are shown in more detail in Figure 33 and 34 below. The events show a hashed identity of the admin and of the organisation tenant, plus the statement that the user is not anonymous (*User.IsAnonymous": false*). This qualification is commonly used as a flag to indicate the user is logged in. Because the test account was logged in, the hashed identities are pseudonymous personal data. Microsoft is technically able to identify the admin.

Figure 33: Example event Office.Taos.Shell.Impression.NavBarFull

```
{
 "name": "Office.Taos.Shell.Impression.NavBarFull",
 "time": "2022-03-29T13:31:26.445Z",
 "ver": "4.0",
 "iKey": "o:b0c82c6598ad49f3848b1d3dc0d8dd25",
 "ext": {
  "sdk": {
   "seq": 1,
   "epoch": "1648560686441",
   "ver": "1DS-Web-JS-3.1.10"
  },
  "metadata": {
   "f": {
    "Event.Sequence": {
      "t": 4
     },
     "Event.Time": {
     "t": 9
     },
     "Data.Impression ItemCount": {
      "t": 6
    }
   }
  }
},
 "data": {
  "baseType": "custom",
  "baseData": {
   "properties": {
     "version": "PostChannel=3.1.10"
   }
  },
  "App.Name": "OfficeTaosShell",
  "App.Platform": "Web",
  "App.Version": "20220325.1",
```

```
"Session.Id": "053e6039-1195-4657-bfb8-7d4a0c4f69e9",
  "Release.AudienceGroup": "Production",
  "User.PrimaryIdentityHash": "1003200138B0D6A3",
  "User.PrimaryIdentitySpace": "OrgIdPUID",
  "User.TenantId": "bd9a989d-e990-4e6e-9566-5a8b29c3b6ff",
  "User.TenantGroup": "Commercial",
  "User.IsAnonymous": false,
  "Context_Env": "NEUprod",
  "Context_Site": "ProtectionCenter",
  "Context SiteSubId": "ShellComplianceCenter",
  "Context WorkloadAppId": "ComplianceCenter",
  "Context PID": "1648560686440 0.24019875064246543",
  "Context_UID": "b2814ab7-0cdb-4b7c-98fe-26deea388bb3",
  "Context_Language": "en-GB",
  "Context Flights":
"15GA,SE404567MyDayOfficeComEnabled,SE404571FetchPhotoUsingGraph,SE404575EnableTe
nantThemeV2,SE404583OfficeHomeVisioStart,SE404593ExchangeDataOpxEnabled,SE404601E
xchangeLoginHint,SE404603OTelTelemetry,SE404609VivaInsightsRollout",
  "Context FlightRings": "WorldWide",
  "Context_Segment": "Dynamics365,Admin,OfficeProPlus,Clp,Teams",
  "Event.Sequence": 1,
  "Event.Name": "Office.Taos.Shell.Impression.NavBarFull",
  "Event.Source": "OTelJS",
  "Event.Time": "2022-03-29T13:31:26.445Z",
  "Data.OTelJS.Version": "4.5.3",
  "Data.Event Type": "Impression",
  "Data.Impression_Name": "NavBarFull",
  "Data.Impression_Category": "NavBar",
  "Data.Impression Context":
"UserTheme:Mountain;ReactVersion:16.10.1;SearchUXEnabled:1;",
  "Data.Impression_ItemCount": 0,
  "Event.Id": "96ccda6f-3ec9-4d58-b318-65760320c14b.1"
 }
```

Figure 34: Example event Office.Taos.Shell.Monitoring

```
},
     "Event.Time": {
      "t": 9
     },
     "Data.Monitoring_AdHoc0": {
      "t": 6
    }
   }
  }
 },
 "data": {
  "baseType": "custom",
  "baseData": {
   "properties": {
     "version": "PostChannel=3.1.10"
   }
  },
  "App.Name": "OfficeTaosShell",
  "App.Platform": "Web",
  "App.Version": "20220325.1",
  "Session.Id": "053e6039-1195-4657-bfb8-7d4a0c4f69e9",
  "Release.AudienceGroup": "Production",
  "User.PrimaryIdentityHash": "1003200138B0D6A3",
  "User.PrimaryIdentitySpace": "OrgIdPUID",
  "User.TenantId": "bd9a989d-e990-4e6e-9566-5a8b29c3b6ff",
  "User.TenantGroup": "Commercial",
  "User.IsAnonymous": false,
  "Context_Env": "NEUprod",
  "Context Site": "ProtectionCenter",
  "Context SiteSubId": "ShellComplianceCenter",
  "Context_WorkloadAppId": "ComplianceCenter",
  "Context_PID": "1648560686440_0.24019875064246543",
  "Context UID": "b2814ab7-0cdb-4b7c-98fe-26deea388bb3",
  "Context_Language": "en-GB",
  "Context_Flights":
"15GA,SE404567MyDayOfficeComEnabled,SE404571FetchPhotoUsingGraph,SE404575EnableTe
nantThemeV2,SE404583OfficeHomeVisioStart,SE404593ExchangeDataOpxEnabled,SE404601E
xchangeLoginHint,SE404603OTelTelemetry,SE404609VivaInsightsRollout",
  "Context_FlightRings": "WorldWide",
  "Context Segment": "Dynamics365,Admin,OfficeProPlus,Clp,Teams",
  "Event.Sequence": 2,
  "Event.Name": "Office.Taos.Shell.Monitoring",
  "Event.Source": "OTelJS",
  "Event.Time": "2022-03-29T13:31:26.447Z",
  "Data.OTelJS.Version": "4.5.3",
  "Data.Event_Type": "TagID",
  "Data.Monitoring_Name": "StorageApi_RequestError",
  "Data.Monitoring_Severity": "Error",
  "Data.Monitoring_AdHoc0": -2007,
  "Event.Id": "96ccda6f-3ec9-4d58-b318-65760320c14b.2"
 }
```

#### 6.2.3 Traffic to Twitter

<u>Figure 35</u> below shows that the Defender Admin Console includes content from Microsoft's Twitter security list. This inclusion leads to the transmission of data to Twitter, as highlighted in yellow in <u>Table 2</u> above. Transmitted data do not include any cookies or unique identifiers, but do include the IP address the admin is connected with.

During the tests Privacy Company was not logged in to Twitter, but even if an admin is logged in to Twitter, Twitter does not collect unique identifiers through cookies or web requests.

<page-header><page-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header>

Figure 35: Microsoft Twitter newsfeed embedded in the Admin Console

# 6.2.4 Traffic to other third parties

Privacy Company also checked if the use of Defender caused other types of thirdparty traffic, including to Microsoft in a role as data controller. In previous reports, a data protection risk was identified related to the use of the Feedback functionality, as the processing of these personal data is not covered by the strict purpose limitation in the privacy amendment with the Dutch government. As shown in <u>Figure</u> <u>36 and Figure</u> <u>37</u> below, Microsoft no longer sends traffic to the third-party services of UserVoice when an admin uses the feedback form.

Figure 36: <u>Headers</u> traffic from Feedback form sent to office.com

ist7calback=_twtr.calbacks.tl_t3_list_Mst5ec _press_response_codes=true	* General						
PostFeedbackData	Request URL: https://portal.office.com/feedback/PostFeedbackData						
PostFeedbackData	Request Method: POST						
i kogstent	Status Code: # 208						
tack	Bannota Addense: 15428-144-1461-481						
ist?calback=_twtt:calbacks.tl_i3_ist_MsftSecpress_response_codes=true	Balana Boline etc. etc. etc. etc. etc. etc. etc. etc						
Ist?calback=_twtr.calbacks.tl_Q_list_MstSecpress_response_codes=true	HERETRY PORCY. STrict-erigin-when-cross-erigin						
	* Response Headers						
	access-control-allow-orsdentials: true						
	access-control-allow-credentials: true						
	access-control-allow-origin: https://security.microsoft.com						
	access-control-expose-headers: +						
	cache-control: no-cache						
	contant-length: 59						
	conteni-type: text/plain; charset=utf=#						
	date: Tue, 29 Mar 2022 14:09:34 GHT						
	expires: -1						
	pragma: no-cache						
	requesi-context: appId=cid=v1:fe512639-39d8-48d1-a28d-1875f814426a						
	set-cookie: s.Sess1D=70736112-fd14-4c8s-b7d1-b87400369261; path=/; secure; HttpDnly						
	set-cookie: s.SessID=7873b112-fd14-4cHa-b7d3-b874803692b1; path=/; secure; HttpDnly						
	sst-cookie: s.cachesap=20; path=/; secure: HttpOnly						
	set-cookim: s_5essID=7872b112-fd14-4cRa-b7d1-b874883557b1; sath=/; secure: HttpOnly						
	sst-cookie: s.cachesap=22; path=/; secure: HttpOnly						
	586-000kim: 5.1.001/N1547Terant126-52YTcbP8x80r19212/BM0020E/+x875467YC10M980021/L0XY715467Y19-842[L154680txdkvi9-4E5+v8Cv4x1Ee+x84xV5hEcCER1FE4v808xx8.012b98771bLbccKh011,NVkDH4E399tHLn						
	6/b5pms; pathw/; secure; HttpDm1y						
	set-cookie: s.DisplayCulture-en-GB: path-/: secure: HttpOnly						
Taxa and AFAR based and AFAR assumed							

Figure 37: <u>Payload</u> traffic from Feedback form sent to office.com

Name	× Headle Payload Neview Response Initiator Timing Cookies
Name Istratiback=_twttr.calbacks.tl (3_list_MsttSecpress_response_codes=true PostFeedbackData PostFeedbackData Occlent track Istratiback=_twttr.calbacks.tl (3_list_MsttSecpress_response_codes=true Istratiback=_twttr.calbacks.tl (3_list_MsttSecpress_response_codes=true)	<pre>X Head: Payload Wriew Response Initiator Timing Cookies VRequest Payload View source *(appl:2281, browser: null, email: null, feature: "homepage@scc",} appl:2281 browser: null email: null feature: "homepage@scc" feedbackType: "5ef14ad=1353-4226-9a37-839e807e74ff" &gt;flight: "proff foo_20120755_EnableServiceAssuranceV2Backend", "DD_20120824_EnableDeviceProtection",] hostAppEm: "proff local: "enapt" page: "https://security.microsoft.com/homepage" page: "https://security.microsoft.com/homepage#" page: "https://security.microsoft.com/homepage#" page</pre>
PostFeedbackData     Occient     vack     tack_tst.tl_3_ist_MsttSecpress_response_codes-true     Ist?calbacks_tst.tl_3_ist_MsttSecpress_response_codes-true	<pre>vapDid: 2281 apDid: 2281 browser: mult, email: mult, reature: -nomepagemeter,, feature: -nomepagemeter -not, email: mult, email: mult email: mult email: mult email: mult feature: -nomepagemeter fights: -nomepagemeter Fights: -nomepagemeter inter page: -notpagemeter page: -n</pre>
	text: "This is a test" userDismissed: false uxVersion: "#"
	version: "5" workload: "AdminPortal"

However, at the bottom of the Feedback form, Microsoft provides a hyperlink to the applicable privacy policy. This link leads to Microsoft's general (consumer) privacy statement, at <a href="https://privacy.microsoft.com/en-us/privacystatement">https://privacy.microsoft.com/en-us/privacystatement</a> .

Figure 38: Reference to Privacy Policy in Microsoft Feedback form

help improve the :	Security Center
late your experience	
****	
Tell us what you liked o	or what we can do better. To protec
your privacy, don't inclu	ude personal information.
You can contact me ab	out this feedback.
] You can contact me ab	out this feedback.
You can contact me ab	out this feedback.
You can contact me ab Floor@PCdpiaTest.c	out this feedback. onmicrosoft.com t
You can contact me ab Floor@PCdpiaTest.c	wout this feedback. on microsoft.com t
You can contact me ab Floor@PCdpiaTest.c	rout this feedback.
You can contact me ab Floor@PCdpiaTest.c Include this screenshot	t Mikuma to Morenth Jab Debuter
You can contact me ab Floor@PCdpiaTest.c Include this screenshol	t Wikewe to Missealt 188 Defeader
You can contact me ab Floor@PCdpiaTest.ct Include this screenshol Include thi	tout this feedback. onmicrosoft.com t Witime to Monant Mit Debuter feedback will be used to improve
You can contact me ab Floor@PCdpiaTest.c Include this screenshol Include this screenshol Inc	nout this feedback.
You can contact me ab Floor@PCdpiaTest.cc Include this screenshol Include this screenshol In	t feedback.
You can contact me ab Floor@PCdpiaTest.c Include this screenshol Include this screenshol Inc	t The formation of the second

#### 6.3 Assessment

It follows from the tests that <u>Microsoft does not automatically send personal data to</u> <u>external third parties</u>. Though Microsoft includes a Twitter feed in the Defender homepage, this does not result in the transfer of personal data to Twitter, except for the IP address, plus the context of the visit to the Defender homepage.

In reply to this verification report, Microsoft acknowledged that the traffic to Twitter was optional. Microsoft has committed to develop an option for admins to centrally block this traffic. Meanwhile, according to Microsoft, users can individually block Twitter content.

Figure 39: Illustration provided by Microsoft for individual removal of Twitter feed

ecurity news feed	
	× Remove
Tweets from @msftsecurity	/
Microsoft Secu 🤣 🍏 @msftsecurity · 2h	Î
Uncover, investigate, and respond to threats in minutes with intelligent guidance informed by 65 trillion	

Microsoft qualifies itself as an independent data controller (and hence, also as a third party) by providing the hyperlink to its (consumer) privacy statement when an admin provides **Feedback**. This is not in line with Microsoft's commitment quoted in the 2022 public DPIA on Teams, OneDrive and SharePoint to stop sending data to third parties once a system administrator had disabled the Controller Connected Experiences.<sup>43</sup> However, the tests in the spring of 2021 showed that Microsoft sent data to itself as data controller (in SharePoint to search engine Bing). Microsoft replied to these findings with a commitment to disable traffic to Bing from SharePoint by mid-2022.

Even though Microsoft has replaced the third party UserVoice with its own customer feedback tools, Microsoft apparently still acts as a data controller for Feedback data. This means Microsoft contractually permits itself to process the personal data resulting from the use of the Feedback option for all seventeen purposes from its (consumer) privacy policy. This includes the display of personalised advertising. See

<sup>&</sup>lt;sup>43</sup> SLM Rijk DPIA on Microsoft Teams, OneDrive, Sharepoint and Azure AD (June 2021, published 16 February 2022, p. 14-15, URL : <u>https://slmmicrosoftrijk.nl/wp-content/uploads/2022/02/Public-DPIA-Teams-OneDrive-SharePoint-and-Azure-AD-16-Feb-2022.pdf</u>

the previous DPIA on Office 365 for the Web and mobile Office apps, as published 30 June 2020, for a full listing of these data controller purposes.<sup>44</sup>

The data processing in and about the use of Feedback is not limited to the three authorised processor purposes. Microsoft has made it possible, through the programming of the Feedback form, that it receives personal data from Enterprise license end-users in a role as data controller. In doing so, Microsoft has at least partially determined the purposes for this data processing. Therefore the organisations and Microsoft can be qualified as joint controllers for the data processing via the Feedback form. Alternatively, if this disclosure does not qualify as joint processing, the Dutch government organisation that allows this data processing is disclosing personal data to a third party. That is a form of 'further processing' for which the organisation is not likely to pass the compatibility test of art. 6(4) of the GDPR.

Microsoft previously argued that it is up to end users (employees) to provide such Feedback, and therefore, that the processing does not pose a high risk for data subjects. This reasoning was not correct. There is no technical blocking option available for Feedback. Hence, organisations can only develop organisational measures such as asking end users not to use the Feedback tool. This is not likely to prevent all data processing by Microsoft, especially since Microsoft does not explicitly warn end users that use of the Feedback form may lead to breaches of work confidential information and/or personal data breaches. Microsoft's mere hyperlink to its (consumer) privacy statement does not provide sufficient warning to admins that they may not use this service.

In reply to this verification report, Microsoft explained that it "*considers an* organization to be the owner of its feedback. Feedback data submitted by an organization's users is viewable and controllable by an organization's administrators."<sup>45</sup>

Microsoft refers to a new information page about the nature of Feedback data processing, the contents, the purposes and how admins can exercise control.<sup>46</sup>

Microsoft writes it collects and processes the Feedback data itself, and only uses it to improve Microsoft products. Microsoft explains: "We get user feedback in the form of questions, problems, compliments, and suggestions. We make sure this feedback makes it back to the appropriate teams, who use feedback to identify, prioritize and make improvements to Microsoft products. Feedback is essential for our product teams to understand our user's experiences, and directly influences the priority of fixes and improvements."

Microsoft acknowledges the processing of Feedback data is completely optional. In reply to this report, Microsoft has committed to make a tenant-level configuration available to centrally disable access to from end users to the Feedback form.

<sup>&</sup>lt;sup>44</sup> DPIA on Microsoft Office 365 for the Web and mobile Office apps, published 30 June 2020, URL: <u>https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps</u>.

<sup>&</sup>lt;sup>45</sup> E-mail Microsoft to SLM Rijk, 14 April 2023

<sup>&</sup>lt;sup>46</sup> Microsoft, Learn about Microsoft feedback for your organization, 17 February 2023, URL: <u>https://learn.microsoft.com/en-us/microsoft-365/admin/misc/feedback-user-control?view=0365-worldwide</u>.

**In sum**, the technical findings show that Microsoft does not share personal data with third parties, except with itself as controller via the Feedback functionality. However, in reply to this verification report, Microsoft has committed to allow its customers to centrally disable Twitter and Feedback.

### 6.4 Remedies

In order to remedy these deviations, <u>Microsoft is advised to take the following two</u> <u>remedies</u>:

- 1. Develop a setting to block the functionality of the Twitter feed
- 2. Develop a group policy or setting to centrally block the use of Feedback in Enterprise and Education tenants or become a data processor.

Additionally Microsoft must be more transparent about the Telemetry Data, but this point will be addressed separately in Section 9 of this report.

• Organisations must use the new technical opt-out functionalities designed by Microsoft to block traffic to Twitter and to Feedback.

# 7. Learnings from security incidents

This section answers the fifth verification question:

Does Microsoft process learnings from security incidents across its Enterprise and Education user base, or are there limitations, such as prior anonymisation?

### 7.1 Facts

Until 2023, Microsoft used the term 'Insights' in its documentation about Cloud App Security and Defender for Endpoint, and wrote that such information could be shared with other customers.<sup>47</sup>

Microsoft explained:

"Customer data is isolated from other customers and is not shared. However, insights on the data resulting from Microsoft processing, and which don't contain any customer-specific data, might be shared with other customers. Each customer can only access data collected from its own organization and generic data that Microsoft provides."48

In order to create the *Insights*, Microsoft explained it removed the identifiers from the data set and qualified the resulting data as `anonymous' data.

In 2020 Microsoft did not provide any access to the Insights in reply to the data subject access request and explained:

<sup>&</sup>lt;sup>47</sup> Microsoft, URL: <u>https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/defender-endpoint/data-storage-privacy.mds</u>.

<sup>&</sup>lt;sup>48</sup> Idem, Answer to the question 'Is data shared with other customers?'

"[T]he resulting data does not retain individual-level identifiers and thus is not personal data."

This statement did not clarify Microsoft's factual processing, as the mere removal of identifiers does not necessarily mean that the remaining data no longer are personal data. There are other ways of reidentifying data, such as when the data can be compared to data from other sources that do contain identifiers, or when the data contains sufficient details to make it possible to zoom in on an individual.

In dialogue with SLM Rijk in April 2023 Microsoft explained that the term Insights was unfortunate. Microsoft has replaced this with the term Threat Intelligence, to clarify that Microsoft only transfers the information about a new threat to its knowledge base of known threats. Microsoft confirmed in writing that it does not process any directly or indirectly identifying personal data for threat intelligence.

Microsoft now explains:

"Customer data is isolated from other customers and is not shared. However, threat intelligence on the data resulting from Microsoft processing, and which don't contain any customer-specific data, might be shared with other customers. Each customer can only access data collected from its own organization and generic data that Microsoft provides."<sup>49</sup>

# 7.2 Technical findings

Privacy Company did not inspect the way Microsoft generates threat intelligence. As mentioned above, and described below, in Section 9, Microsoft did not provide any data about the Insights in reply to the data subject access requests

# 7.3 Assessment

Microsoft's explanation and improved public explanations have removed a potential data protection risk of further processing of pseudonymised personal data about security threats at individual customers and users outside of the customer tenant.

The processing of some pseudonymised personal data at an aggregated level (never on a per tenant basis) for the purpose of providing a secure service is not problematic. First of all, based on Articles 28 (3) sub c and 32 of the GDPR Microsoft necessarily has to process some personal data to comply with its legal obligations as a processor to protect the personal data entrusted to it by its customers with appropriate technical and organisational measures to ensure a level of security appropriate to the (global) risks. This for example includes developing and delivering security updates for all customers, based on an inventory of global threats.

Contractually the Dutch government and universities have agreed that Microsoft may 'further' process limited personal data as independent data controller for a limited list of legitimate business purposes, when proportionate.

One of these purposes is combatting fraud, cybercrime and cyber-attacks that may affect any Microsoft product or service. Microsoft has explained to SLM Rijk that it

<sup>&</sup>lt;sup>49</sup> Microsoft Defender for Endpoint, Is data shared with other customers?, 8 February 2023, URL: <u>https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/data-storage-privacy?view=o365-worldwide#is-data-shared-with-other-customers</u>

"does not and has not processed any security related personal data for the agreed Legitimate Business Operations purpose."<sup>50</sup>

According to the privacy amendment negotiated by SLM Rijk with Microsoft, as a processor Microsoft may only process personal data to the extent necessary, and otherwise rely on pseudonymised aggregated data. The obligation to provide a secure service legitimises that Microsoft 'learns' from security incidents across its customer base, based on pseudonymised data, to develop mitigating measures such as security updates and to inform all customers about detected threats and recommended measures.

Additionally, the Dutch government and universities' privacy amendment allows Microsoft to 'further' process some personal data to combat fraud, cybercrime, or cyberattacks in a role <u>as data controller</u>, for Microsoft's own legitimate business purposes. In this 'controller' role, Microsoft is contractually prohibited from reidentifying pseudonymised or de-identified personal data.

In reply to this verification report Microsoft explained the use of the word 'Insights' was unfortunate. The processing only involves transferring information learned from new threats to the list with 'known threats' Insights do not include any personal data from customers, but identify for example malware, or a malicious URL used for phishing. Microsoft has updated its information on 3 April 2023. The word "Insights" was removed and replaced with the term "threat intelligence". Microsoft explicitly documents that threat intelligence does not include any personal data from customers.<sup>51</sup>

Microsoft has also explained it does not and has not processed any security-related personal data for the agreed Legitimate Business Operations of combatting fraud, cybercrime or cyberattacks.<sup>52</sup>

An additional (security) risk is that Microsoft does not aggregate the information about the threat on a sufficiently high level to prevent leakage of critical cyber security information. For example, Microsoft recently published a threat advisory about Russian attacks on organisations in Ukraine spanning government, military, NGOs, judiciary and law enforcement and not-for-profits.<sup>53</sup> If Microsoft would publish a similar advisory about an attack on Dutch government institutions, this information could compromise investigations by the security services.

In reply to this possible risk, Microsoft explained "All data transferred to the United States is maintained in protected data stores with controls to ensure that it is only processed for permitted purposes."<sup>54</sup>

<sup>&</sup>lt;sup>50</sup> E-mail Microsoft to SLM Rijk, 31 March 2023.

<sup>&</sup>lt;sup>51</sup> E-mail Microsoft to SLM Rijk, 14 April 2023.

<sup>&</sup>lt;sup>52</sup> Idem.

<sup>&</sup>lt;sup>53</sup> Microsoft ACTINIUM targets Ukrainian organizations, 4 February 2022, URL: <u>https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/</u>

 $<sup>^{\</sup>rm 54}$  E-mail Microsoft to SLM Rijk, 14 April 2023.

# 7.4 Remedies

Following Microsoft's explanations there are <u>no recommendations for Microsoft or for</u> <u>organisations</u>.

# 8. Risk profiles

This section answers the sixth verification question:

Does Defender create individual risk profiles and/or individual scores in the different analytic overviews and reports?

#### 8.1 Facts

As summarised in the Introduction Defender offers a wide variety of risk detection tools. Most of these tools are focussed on the occurrence and nature of the threats, not on individual users. There are two specific resources that show individual risk scores (i) Users at risk and (ii) Top targeted users. Besides, admins can always zoom in to the level of individual users, mailboxes or devices and create their own profiling logic.

Defender registers behaviour within Office and the Azure AD, and classifies some behaviour as risky, such as a suspicious login, clicking on a phishing link or receiving malware. The resources with 'profiles' thus consist of either passive or active risky behaviour.

As described in Section 4.1 (Detection of suspicious logins in the Azure AD) Microsoft monitors historical user login activity to warn about suspicious logins.

Microsofts overview of 'Users at risk' is based on 19 threat detection types, as shown in two screenshots in <u>Figure 40</u> below.

Figure 40: Microsoft	detection	types
----------------------	-----------	-------

etection type(s) : None Selected	Detection type(s) : None Selected
Detection type(s)	Detection type(s)
Activity from anonymous IP address	Nation state IP
Anomalous token	New country
Anonymous IP address	Password spray
Atypical travel	Possible attempt to access Primary Refresh Token
Azure AD threat intelligence	(PRT)
Impossible travel	Suspicious browser
Malicious IP address	Suspicious inbox forwarding
Malware linked IP address	Suspicious inbox manipulation rules
Mass access to sensitive files	Suspicious sending patterns
Nation state IP	Token issuer anomaly
New country	Unfamiliar sign-in properties
Annels	Apply

These different threat types describe generic assumptions about threats, such as an impossibly short travel time between two geolocations. The tests did not provide any indication that Defender identifies threats based on deviations of individual end user profiles. In other words, the risk profiles reflect 'known' bad behaviour patterns, as applied to individual users, but not individual behavioural profiles.

There are two apparent exceptions to this rule: (i) *Atypical travel* and (ii) *Unfamiliar sign-in properties*.

Machine learning is applied to detect 'atypical travel'. Microsoft explains that this risk is based on a combination of geographically distant locations and past user behaviour.

Microsoft writes:

"This risk detection type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behaviour. Among several other factors, this machine learning algorithm takes into account the time between the two sign-ins and the time it would have taken for the user to travel from the first location to the second, indicating that a different user is using the same credentials.

The algorithm ignores obvious "false positives" contributing to the impossible travel conditions, such as VPNs and locations regularly used by other users in the organization. The system has an initial learning period of the earliest of 14 days or 10 logins, during which it learns a new user's sign-in behaviour."<sup>55</sup>

The detection of unfamiliar login properties is based on a profile of the login history of a specific user and behaviour of other employees in that organisation. For example: a user logging in from a country he has never logged in from before. Microsoft may not qualify such a login as a risk if logins from that country are common for that organisation.

The second resource with user risk profiles is a tab in Explorer, as described in Section 1.5.3 of this report. This shows a graph of the 'Top targeted users', the end users that most frequently receive suspicious mails (with malware or phishing links). See <u>Figure 13</u> above.

Microsoft writes in the Azure Active Directory Data Security Considerations:

"Azure AD Identity Protection uses real-time user login data **along with multiple signals from company and industry sources to feed to its machine learning systems to detect anomalous logins.** Personal data is scrubbed from this real-time login data before it is passed into the machine

<sup>&</sup>lt;sup>55</sup> Microsoft, Premium sign-in risk detections, 20 April 2022, URL: <u>https://docs.microsoft.com/en-gb/azure/active-directory/identity-protection/concept-identity-protection-risks#premium-sign-in-risk-detections</u>

learning system, along with the remaining login data used to identify users and logins that are potentially risky."  $^{\rm 756}$ 

The emphasised words suggest that Microsoft uses information from external sources. However, in reply to this report, Microsoft has confirmed in writing that it does not.

"Microsoft Defender for Endpoint does not use external risk profiling sources to prevent malicious login attempts. The service only uses/combines the personal data obtained by several Defender services used within one tenant, and only for the purpose of providing these services to the Customer."<sup>57</sup>

Admins can use the information about this labelled 'risky' behaviour to determine the threshold for decisions on individual users. As described in Section 1.5.4 of this report, Review asks admins to decide what to do with users that have been blocked by Microsoft for sending too many messages classified as bulk mail. See <u>Figure 16</u> above.

For example: if a specific user receives malware, Microsoft automatically puts the mail in a quarantine folder. Admins can decide if they allow end users to view the quarantined mails, or not.

#### 8.2 Technical findings

Privacy Company did not inspect the data processing performed by Microsoft inside the Defender services. As shown in Section 9, about the results of the data subject access requests filed for this verification report, Microsoft did not provide any data about the algorithms used to assign a risk score.

#### 8.3 Assessment

Defender needs to process data from Microsofts raw logs such as locations of users' logins, device information and IP addresses to detect and mitigate risks and threats. Defender needs to have a flexible data processing scope to detect new and emergent risks. Defender also enables the admins to proactively hunt for risks specific to the organisation. The admins therefore also have a flexible data processing scope.

It is reassuring that Microsoft provides a description of its detection algorithms and the specific risk profiles that are applied. The descriptions are aimed at admins, not at end users. To ensure that the employees and students understand the nature of the data processing, organisations must bridge the information gap and explain in more accessible language what Microsoft does and does not do with user behaviour data, and how the organisation uses the risk profiles and alerts.

## 8.4 Remedies

With regard to the risk profiles organisations are advised to take the following remedy:

<sup>&</sup>lt;sup>56</sup> Microsoft, Azure Active Directory Data Security Considerations, 1 July 2020, p. 11, URL: <u>https://azure.microsoft.com/en-us/resources/azure-active-directory-data-</u> <u>securityconsiderations/</u>.

<sup>&</sup>lt;sup>57</sup> E-mail Microsoft to SLM Rijk, 18 April 2023.

 Provide a concise, intelligible and easily accessible internal explanation to employees about the data processing in Defender

# 9. Quality of public information

This section answers the seventh verification question:

Does Microsoft publish adequate documentation on the personal data it collects through the tested applications, in comparison with captured network traffic and logs that are accessible for system administrators??

### 9.1 Facts

As data processor for Microsoft 365 Enterprise (and Education), Microsoft must assist the data controllers (the Dutch government organisations and universities) with their obligation to adequately inform end users about the data processing, based on Art. 14 of the GDPR.

Microsoft does publish documentation about the nature of the data processing through Defender and an introduction to the concept of 'risk'. Until 2023 Microsoft provided limited information about the retention periods and did not publish information about the Telemetry Data it collects from browsers from admins when they use the admin portal.

Microsoft only provided brief information about the retention periods in a FAQ for admins.  $^{\rm 58}$ 

- "The risky users view shows a user's risk standing based on all past signins.
- The risky sign-ins view shows at-risk signs in the last 30 days.
- The risk detections view shows risk detections made in the last 90 days."

As shown in <u>Figure 41</u> below, the default retention period for the sign-ins is 180 days (based on Defender for Endpoint settings).

<sup>&</sup>lt;sup>58</sup> Microsoft, How far can I go back in time to understand what's going on with my user?, URL: <u>https://docs.microsoft.com/en-gb/azure/active-directory/identity-protection/troubleshooting-identity-protection-faq#how-far-can-i-go-back-in-time-to-understand-whats-going-on-with-my-user</u>.

Figure 41: Default retention period

Data Retention		
This will determine the peri Note this does not refer to For more information, see t	od of time we retain your data in your clo expiration or cancellation of your Microso ne <b>Data storage and privacy</b> section in t	ud instance. ft Defender for Endpoint contract. he Microsoft Defender for Endpoint guide.
180 days	~	

In 2023 Microsoft has improved transparency about the specific personal data it collects through the four investigated tools, and the data retention periods.

# 9.1.1 Retention periods in Defender for Office 365

By default, Microsoft retains the Defender for Office 365 data for a maximum of 30 days. Depending on the type of Plan the customer has, data can be retained up to 180 days for the Action Center.<sup>59</sup>

# Figure 42: Microsoft table of retention periods in Defender for Office 365<sup>60</sup> Defender for Office 365 Plan 1

Feature	Retention period
Alert metadata details (Microsoft Defender for Office alerts)	90 days.
Entity metadata details (Email)	30 days.
Activity alert details (audit logs)	7 days.
Email entity page	30 days.
Quarantine	30 days (configurable; 30 days is the maximum).
Reports	90 days for aggregated data.
	30 days for detailed information.
Submissions	30 days.
Real-Time detections	30 days.

### 9.1.2 Retention periods in Defender for Endpoint

Microsoft writes that data from Microsoft Defender for Endpoint are "*retained for 180 days, visible across the portal. However, in the advanced hunting investigation experience, it is accessible via a query for a period of 30 days.*"<sup>61</sup>

Microsoft describes that it stores the Defender for Endpoint data "*in a customer dedicated and segregated tenant specific to the service for administration, tracking, and reporting purposes.*"<sup>62</sup>

<sup>&</sup>lt;sup>59</sup> Microsoft, Data retention information for Microsoft Defender for Office 365, 13 March 2023, URL: <u>https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention?view=0365-worldwide</u>.

<sup>60</sup> Idem.

<sup>&</sup>lt;sup>61</sup> Microsoft, Microsoft Defender for Endpoint data storage and privacy, 8 February 2023, URL: <u>https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/data-storage-privacy?view=0365-worldwide</u>

<sup>62</sup> Ibid.

The data include: "file data (such as file names, sizes, and hashes), process data (running processes, hashes), registry data, network connection data (host Ips and ports), and device details (such as device identifiers, names, and the operating system version)."<sup>63</sup>

9.1.3 Retention periods in Defender for Cloud Apps Microsoft discerns between 4 types of logs.

"Activity log: 180 days

Discovery data: 90 days

Alerts: 180 days

Governance log: 120 days"64

9.1.4 Retention periods Defender for Identity

Microsoft does not publish separate retention periods for Defender for Identity. as these periods are related to the retention periods for the Azure AD determined by the organisations. Microsoft only mentions the retention period of 90 days for the audit log.

"Defender for Identity implements the audit of personal data changes, including the deleting and exporting of personal data records. Audit trail retention time is 90 days. Auditing in Defender for Identity is a back-end feature and not accessible to customers."<sup>65</sup>

Additionally, Microsoft does not publish information about the two types of Telemetry Data described in Section 6.2 of this report: the traffic to the analytical subdomains and the traffic to the two known telemetry domains. The contents of this traffic are limited because the data only relate to the use of the admin portal.

## 9.2 Technical findings

The intercepted Telemetry Data are described in Sections 6.2.1 and 6.2.2. As described above, Microsoft does not publish documentation about this category of personal data. Microsoft also did not provide access to these data in response to a Data Subject Access Request. This will be specified in Section 10 of this report.

#### 9.3 Assessment

Microsoft generally collects the personal data it processes in Defender in an indirect manner (observed behaviour). This means Microsoft must enable its customers to comply with the indirect information obligation from Art. 14(1) sub d of the GDPR As data processor, Microsoft is obliged to comply with art 28(3) sub e of the GDPR, and

<sup>63</sup> Ibid.

<sup>&</sup>lt;sup>64</sup> Microsoft, Data security and privacy practices for Defender for Cloud Apps, 24 April 2023, URL: <u>https://learn.microsoft.com/en-us/defender-cloud-apps/cas-compliance-trust#data-retention</u>.

<sup>&</sup>lt;sup>65</sup> Microsoft Defender for Identity, Microsoft Defender for Identity data security and privacy, 5 February 2023, URL: <u>https://learn.microsoft.com/en-us/defender-for-identity/privacy-</u> <u>compliance/</u>.

assist its Enterprise customers with the exercise of data subjects rights such as the right to information.

Microsoft does not provide the required assistance with regard to the retention periods and the Telemetry Data.

### 9.4 Remedies

In order to remedy the lack of transparency, <u>Microsoft is advised to take the</u> <u>following remedy</u>:

• Microsoft must provide more information about the observed Telemetry Data from the admin portal, unless Microsoft is able to ensure that the browser telemetry data do not contain any identifying (pseudonymous) personal data.

# **10.** Data Subject Access

This section answers the (eight) verification question:

Does Microsoft give system administrators full access to all personal data it processes through the different Defender tools? Does Microsoft provide adequate explanations if it does not provide access to certain personal data?

# 10.1 Facts

Microsoft offers two different tools for data subject access requests:

- 1. A DSAR tool to retrieve Content Data from a specific user.<sup>66</sup> This tool was renamed in September 2021 to User data search.<sup>67</sup>
- 2. A DSAR tool to retrieve Diagnostic Data from a specific user.<sup>68</sup>

This first tool (shown in Figure 43 and Figure 44) only provides access to Content Data in SharePoint, Exchange and Teams. That information does not specifically relate to any security processing by Microsoft and is therefore not useful for this report. Additionally, the export does not contain any files stored in OneDrive, while malicious files such as the Eicar test-file were stored in OneDrive, and cannot be retrieved via this portal.

<sup>66</sup> Microsoft, Data Subject Requests, Part 1: Responding to DSRs for Customer Data, Using the Content Search eDiscovery tool to respond to DSRs, URL: <u>https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Office365#part-1-responding-to-dsrs-for-customer-data</u> <sup>67</sup> Microsoft, User Data Search, URL: <u>https://compliance.microsoft.com/userdatasearch</u>

<sup>&</sup>lt;sup>68</sup> Microsoft, Data Subject Requests, Part 3: Responding to DSRs for system-generated Logs, URL: <u>https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Office365#part-3-</u> <u>responding-to-dsrs-for-system-generated-logs</u>. This tool can only be used by the tenant admin.

	•			Win 10 Pro EOP ATP	(Updates geinst	alleerd (2022-03-3	0)) [Running]		
	A Floor Terra - Export - Microsoft	tix 🤹	Algemeen (Floor Terra - Export) 🛛 🗙   +					-	σ×
~	O D https://ce	ompliance.mi	crosoft.com/privacymgmtsrm/entity/6e022f1d-r	a2d-4841-a444-22a3	1560404#?entityn	ame = Floor%20Terral	1620-1620ExportBientityviewid=datacollected AN 0A 😘 🏠		B
ш	Microsoft Purview	-			-	2		0	? 🗇
田田	Catalog App governance		Privacy management: Subject rights requests	> Floor Terra - Expo	rt.		🖉 Edit 🙄 Close the request 📫 Chat with collaborators (28 Automate ~	년 Share	~
10	Audit		Floor Terra - Export Sta	pe 4 of 5 - Generate i	reports		Close	the reques	it.
P	Content search		Overview Data collected Notes	Collaborators	Reports				
63	Communication compliance								
6	Data loss prevention		Filter 😤 Reset 🦉 Filters						
兪	eDiscovery	~	Location: Any 😪 Review status: Any	Tags: Any 🗠	Content own	nen Any 🗠			
	Data lifecycle management		Location SharePoint	columna 🛓 Expo	rt 🕐 Refresh	100 items	Subject line	×	
0	Information Register		Teams	Review status	Tags.	Content owner			
A	Insider risk management		Schemoprame (51) prg	Not reviewed	Not tagged	0 floor			
Q.	Records management		E3 Easter Day	<ul> <li>Not reviewed</li> </ul>	Not tagged	Floor Ter			
	Priva Privacy Risk Managem	~	Screenshot 2021-09-27 at 16.06.02.pr	g • Not reviewed	Not tagged	0 floor			
1 62	Priva Subject Rights Requests		Weekly digest: Microsoft service update	<ul> <li>Not reviewed</li> </ul>	Not tagged	Microsof	Select an item from the list to preview its content		
0	Sattinos		ES Thankspiving Day	<ul> <li>Not reviewed</li> </ul>	Not tagged	Floor Ter			0
0	More resources		Schermopname (24) prg	<ul> <li>Not reviewed</li> </ul>	Not tagged	0 floor			(CDI)
			Tax Day	<ul> <li>Not reviewed</li> </ul>	Not tagged	Floor Ter			
0	Customize navigation		1			,			
-	,P Typ hier om te zoeken		0 🕸 💽 🖬 🖬				B Nuregen 수 현 60 단	(1) 15:40 20-4-30	222 💭

# Figure 43 Export of Content Data from SharePoint, Exchange and Teams

# Figure 44: Content export tool does not find Eicar test file in OneDrive

	8 Floor Tena - Export - Microso	n x	🔒 Algemeen (Flo	oor Terra - Export   X   +										-	o x
~	→ C @ https://	compliance	microsoft.com	/privacymgmtsrm/entity/6	e022/1d-ca2d-4541-a444-22a35604	404mentityname=Floor%2	Terra%20-%208	portBantityviewid	datact	flected	Ab	08 12	1	۵	
	Microsoft Purview						~		2	<b>e</b> -	_			0	? (
田田鹿の	Catalog App governance Audit Content search		Privacy m Floor Overviev	anagement: Subject rights <b>r Terra -</b> Expo w Data collected	requests > Roor Terra - Export rt Stage 4 of 5 - Generate repor Notes Collaborators Rep	rts xorts		' Edit 🖨 Close ti	w requ	est 🜒 Chat with	i collaborators	(R Aut	omate V Close	년 Sha the requ	re ~
CG CG 4	Communication compliance Data loss prevention eDiscovery	2	Filter 12	Reset 😨 Filters Any 💛 Review stats	a: Any 🗸 Taga: Any 🗸	Content owner. Any 😪									
	Data lifecycle management Information protection		eist.	× =	Customize columns 🛓 Export 🔇	) Refresh			-		Maddled dat			5 ite	ms.
2	Information Barriers Insider risk management	~	> =	Undeliverable: Floor Terra	shared "eicar" with you.		Not reviewed	Not tegged	•	Microsoft Ou	16 New 2021	15.35	Ex	change	
8	Records management Priva Privacy Risk Managem	~		3 Test eicar via onedrive			Nat reviewed	Not tagged	•	Roor Terra	16 Nov 2021	15:13	b	change	
0	Priva Subject Rights Requests Settings			<ol> <li>Picor Terra shared "eicar"</li> <li>Bicar test</li> </ol>	ette you.		Not reviewed     Not reviewed	Not tagged	•	Floor Terta	16 Nov 2021 4 Apr 2022 16	15.35	Ex.	change change	0
0	More resources Customize navigation														Ø
-	P Typ hier om te zoeken			o # 💽 I	a 💼 💼					<u>-</u> Q	😑 16°C Zon	nig 🔨	ê 10 C	1 di) 10 10	-3022

The second tool is relevant for this report. As shown in <u>Figure 45</u> below, Microsoft explains that the admin needs to create a separate Azure blob. The use of Azure storage is not included in the (most expensive) E5 Enterprise license.

#### Figure 45: Microsoft explanation of the DSAR tool for diagnostic data

To access and export system-generated logs:

- 1. Sign in to the Azure portal and select All services.
- 2. Type policy into the filter, and then select **Policy**.
- 3. In the Policy blade, select User privacy, select Manage User Requests, and then select Add export request.

4. Complete the Export data request:

- User. Type the email address of the Azure Active Directory user that requested the export.
- Subscription. Select the account you use to report resource usage and to bill for services. This is also the location of your Azure storage account.
- Storage account. Select the location of your Azure Storage (Blob). For more info, see the Introduction to Microsoft Azure Storage Blob storage article.
- Container. Create a new (or select an existing) container as the storage location for the user's exported privacy data.

#### 5. Select Create.

The export request goes into Pending status. You can view the report status on the User privacy > Overview blade.

#### (i) Important

Because personal data can come from multiple systems, it's possible that the export process might take up to one month to complete.

Microsoft explains that an export usually takes 1 or 2 days, but may take up to 20 days. Microsoft warns that exported data "*do not include data that may compromise the security or stability of the service.*"<sup>69</sup> This warning corresponds with Microsoft's earlier statement that *service-related event level information regularly includes confidential security or other proprietary information about the operation of our services, where publication of such data could put our services, and thus our customers and Microsoft, at risk.*"<sup>70</sup>

Microsoft publicly commits to provide access to the *Required Service Data* in response to a Data Subject Access Request.

Figure 46: Microsoft commitment to provide Data Subject Access<sup>71</sup>

Required service data is available through Data Service Requests (DSRs). For more information, see the Microsoft Privacy Statement <sup>™</sup> and Office 365 Data Subject Requests for the GDPR and CCPA.

#### **10.2** Technical findings

In 2020 Privacy Company filed data subject access requests about Cloud Apps Security (now; Defender for Cloud Apps) and about Defender for Endpoint. Microsoft responded that only the given identifier was found in their systems, but no other personal data was discovered.

<sup>&</sup>lt;sup>69</sup> Microsoft, What data do the export results return?, URL: <u>https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Office365#part-3-responding-to-dsrs-for-system-generated-logs</u>

 <sup>&</sup>lt;sup>70</sup> Microsoft reply to Teams, OneDrive and SharePoint DPIA for SLM Rijk, 27 June 2021.
 <sup>71</sup> Microsoft, Required service data for Office, 30 September 2021, URL: https://docs.microsoft.com/en-us/deployoffice/privacy/required-service-data

This answer was in contrast with the intercepted network data sent by Defender for Endpoint and used by Cloud Apps Security, as well as known data sources in connection with Azure AD.

In correspondence following these 2020 data access requests, Microsoft stated that it did not have any personal data, since it deidentifies, pseudonymises and aggregates the data in compliance with ISO/IEC 19944 standards. Microsoft also argued the Device ID was not personal data, as it could only be linked to a device, not to an individual.

The DSAR exercised in 2022 for Office 365 and Defender for Identity resulted in an export to an Azure Blob Container and contains a large amount of files. Each of these files may contain many different events (actions) for different applications, but with a different structure, and often with incomprehensible random strings of characters as file names.

It took Microsoft one month to complete the DSAR request. The request was filed on 20 April 2022, and the request was completed on 20 May 2022.

Privacy Company performed a search for the observed telemetry events in the DSAR results and could not identify any of the observed events.

Microsoft does not provide any explanation about the exported results, nor a tool to structure or query the contents per app, per action or per time period. There is no explanation about types of information that has been withheld for security or confidentiality reasons.

The DSAR tool doesn't allow for filtering based on time and does contain events from outside the scripted test-scenario's, for example events on the use of Teams prior to this technical verification report, in the same tenant ID.

Filename	Size (bytes)
RequestInfo.json	641
c6df84882b434278bf2a0f6517a52c68/3134bf67a6a9405fb3344e5f 287f7e87/1010/Microsoft365_Outlook_OWA_ProductAndServiceUs age.json	575
2dbe5f8b339840ac9bced223f8817843/3134bf67a6a9405fb3344e5f 287f7e87/commandId.txt	165
ca137276a7ac45458db97477cd0100db/3134bf67a6a9405fb3344e5 f287f7e87/1565/ProductAndServiceUsage_OfficeApps.json	2115802
e611d051f7af45b6af02964e88f4d7aa/3134bf67a6a9405fb3344e5f 287f7e87/commandId.txt	165
08f660c9975847a4a19af2c90512c5cf/7b35fc36d9b54e468b6a78d8 46a9edb5/1005/ProductAndServiceUsage.json	180586
a4370d95fb614032be19072360bb9552/6a3113dcd76843338eba15 69035bd46f/1005/Microsoft365_AdminCenter_Microsoft365_Admin Center_Online_Account_UserLoginInfo.json	178
a4370d95fb614032be19072360bb9552/6a3113dcd76843338eba15 69035bd46f/1005/Microsoft365_AdminCenter_Microsoft365_Admin Center_Online_Account_RememberPreferences.json	296

Table 6: DSAR Export results

a4370d95fb614032be19072360bb9552/6a3113dcd76843338eba15	334
60035bd46f/1005/Microsoft365_AdminContor_Microsoft365_Admin	554
Canton Online Account WhateNewDreferences icon	
	110
a43/0d95fb614032be190/2360bb9552/6a3113dcd/6843338eba15	118
69035bd46f/1005/Microsoft365_AdminCenter_Microsoft365_Admin	
Center_Online_Account_MagicCarpetUserPreferences.json	
a4370d95fb614032be19072360bb9552/6a3113dcd76843338eba15	89
69035bd46f/1005/Microsoft365 AdminCenter Microsoft365 Admin	
Center Online Account FeatureExplorerViewModePreferences.ison	
a4370d95fb614032be19072360bb9552/6a3113dcd76843338eba15	255
60035hd/6f/1005/Microsoft365_AdminCenter_Online_CustomerCo	200
ntent TID BD04090D E000 4E6E 0E66 E49B20C2B6EE icon	
95e26a9d512c4f02a3fd813765995c89/e7cd9bc9a1d14c56977ad40	4
227589995/1005/Feedback And Ratings.json	
00d56b4a81e04279ac3a9b7f036e1d5a/76cadbc9b7774b54be2194	4
ca0b631c36/0/ProductAndServiceUsage.json	
400eccd00d6449e7a1799a361d158bd8/0614e334db47470498116c	248
e4fa328e36/225/ProductAndServiceUsage_ison	
6970f241ab054064844c106e1d200cb2/3134bf67a6a9405fb3344e5	101
f297f7a97/1010/Microsoft265 Evolution Outlook Addin Store Drodu	797
120/1/e0//1010/Microsoft305_Exchange_OutlookAddinStore_Produ	
ctAndServiceUsageData_1.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	15162
5a821f7/12711242.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	43519
5a821f7/3517510.ison	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	43004
5-821f7/3868816 icon	-300-
2422Ed9f0c0944210EEd0124c24bE226/c914ff92c1224f900ff2d7fc0	126442
	120442
58821F//10042482.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d/fa0	138696
5a821f7/3759676.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	8591
5a821f7/9569148.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	776562
5a821f7/72166.ison	
a42a5d8f0c984421955d01a4a24b5336/c814ff83c1324f809ff3d7fa0	150207
5-821f7/1171/202 icon	130207
30211//11/14203.j5011	1100004
	1166084
588211//3382983.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	311
5a821f7/15569482.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	8764
5a821f7/253221.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	26835
5a821f7/3575199 ison	20000
2422Ed9f0c0844210EEd0124224bE226/c814ff82c1224f800ff2d7f20	100074
a42a3u010C904421933u01a4e24b3330/C0141103C13241009113u71a0	190974
	1 1 2 2
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d/fa0	1489
5a821t7/10520228.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	348122
5a821f7/8725734.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	5107364
5a821f7/192269.ison	
a42a5d8f0c984421955d01a4a24b5336/c814ff83c1324f800ff3d7fa0	784
52821f7/252220 icon	707
Jaozii//2JJZZU.jSUII	2062
	3002
538211//4584684.JSON	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	87417
5a821f7/13584527.json	

a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	194207
5a821f7/9835187.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	33276
5a821f7/13148361.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	62403
5a821f7/3590448.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	48679
5a821f7/192242.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	290307
5a821f7/2385068.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	781
5a821f7/12834694.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	46586
5a821f7/11714213.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	471991
5a821f7/10653902.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	129657
5a821f7/11666262.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	721
5a821f7/3655985.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	12372
5a821f7/12124541.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	47736
5a821f7/283666.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	216748
5a821f7/3575202.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	20338
5a821f7/14610187.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	86793
5a821f7/2748875.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	1155
5a821f7/3922370.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	2301
5a821f7/111276.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	8764
5a821f7/3590445.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	14436
5a821f7/3389599.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	471
5a821f7/13247049.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	750
5a821f7/9923815.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	218595
5a821f7/10830189.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	1637
5a821f7/13419687.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	48534
5a821f7/286128.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	321746
5a821f7/13148329.ison	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	6183
5a821f7/4569249.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	743
5a821f7/13267215.json	-

a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	202248
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	125376
5a821f7/192276.json	123370
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	207706
5a821f7/3575200.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	743
5a821f7/6328826.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	4488
5a821f7/12883190.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	6691
5a821f7/2162603.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	750
5a821f7/10487448.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	855
5a821f7/3518376.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	393
5a821f7/9569208.json	704
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d/fa0	/84
58821F//3590450.json	2067021
a42a508f0C984421955001a4e2405336/C814ff83C1324f809ff30/fa0	2867031
3do211//3/33300.JS011 2422Ed9f0c0944210EEd0124c24bE226/c914ff92c1224f900ff2d7f20	2542
5a821f7/4830768 ison	2343
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	1711
5a821f7/647652 ison	1/11
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	6048778
5a821f7/13259472.ison	0010770
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	24246
5a821f7/4569511.json	-
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	12573578
5a821f7/11714206.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	9156
5a821f7/8375687.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	521
5a821f7/13252635.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	11811914
5a821f7/10748310.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	78312
58821f7/2385483.json	122555
a42a508f0C984421955001a4e2405336/C814ft83C1324f809ft30/fa0	128666
3do211//4002107.j5011 2422Ed8f0c0844210EEd0124c24bE226/c814ff82c1224f800ff2d7fa0	240400
442d5u010C904421955u01d4024D5550/C0141105C15241009115u71d0	249490
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	493495
5a821f7/12670722 ison	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	102182
5a821f7/10584507.ison	102102
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	6165
5a821f7/11557923.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	14844
5a821f7/12015245.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	5409
5a821f7/4581962.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	8293
5a821f7/13356765.json	44.000
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	418091
5a821t//9837044.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	1128
--	---------
5a821f7/3389420.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	2791567
58821f//3656010.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	6038
5a821f7/10525443.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	2805454
5a821f7/3656011.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	445650
5a821f7/11714216.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	1881
5a821f7/3742824.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	8786
5a821f7/11714236.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	869
5a821f7/13607420.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	786
5a821f7/13219196.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	917
5a821f7/9562245.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	521
5a821f7/13247057.json	
a42a5d8f0c984421955d01a4e24b5336/c814ff83c1324f809ff3d7fa0	17104
5a821f7/10265806.json	
135e4fd3170e4b44beb0b270c60f289e/7b35fc36d9b54e468b6a78d	180586
846a9edb5/1005/ProductAndServiceUsage.json	
af1378eb1f7a4fcdb7c3b2cb71053bb5/efde18ca75354e008cf4fa343	165
e3e7b31/commandId.txt	
bfd06a9ff6e243ffaf0b13f385768313/7b35fc36d9b54e468b6a78d84	180586
6a9edb5/1005/ProductAndServiceUsage.json	
ea3537d4ba704f589610a4a7a8a8e8a8/7b35fc36d9b54e468b6a78	180586
d846a9edb5/1005/ProductAndServiceUsage.json	
ba149b6472004e638175b98ca076318c/3134bf67a6a9405fb3344e	165
5f287f7e87/commandId.txt	
abab1cc2bcac4dbd9d4018a387fe7637/3134bf67a6a9405fb3344e5f	165
287f7e87/commandId.txt	
d364c307aafe4289b78b28125a20e3aa/3134bf67a6a9405fb3344e5	165
f287f7e87/commandId.txt	
37a0e5bcebe0456d907041c22341ed81/3134bf67a6a9405fb3344e	165
5f287f7e87/commandId.txt	
a0c8f27fe183466b820da95d8be178dd/3134bf67a6a9405fb3344e5f	165
287f7e87/commandId.txt	

Microsoft provides two types of DSAR files: the first category contains information about the individual use of services. The second category is 'other', with many different types of information.

### First category

The first category is called 'ProductAndServiceUsage'. These are not the Telemetry Data sent from the end user browser or device, but the Diagnostic Data directly generated by Microsoft itself, on its cloud servers. None of these events contain any information relating to the use of Defender. Therefore, these data are out of scope of this report. The only type of events in this category are log-ins of the admin to the Azure AD, as shown in Figure 47 below. Directly identifiable data in this event have

partially been pseudonymised or replaced with generic terms such as 'REDACTED' or 'POSSIBLE\_ARM\_OBJECT\_ID', but the tenant domain and userDisplayName are still transferred in the clear, as highlighted in yellow.

Figure 47: Example of event related to use of Azure AD



#### Second category

It is not possible to summarise the contents of the other types of events provided in reply to the DSAR request with a few common characteristics.

The Telemetry Data are encoded in several different formats, but the structure of each event is always similar. Each outgoing event in the data traffic has a header of standardised fields, and some contents that are unique for that type of event. The header contains the event name, date and timestamp and some other fields. That makes it possible to analyse the entire flow of Telemetry Data by event type.

The DSAR files in this second category however do not contain any such headers or otherwise identifiable common structure to distinguish per event type. Therefore, it is not possible to structurally compare the observed outgoing Telemetry Data with the results in this second category.

Privacy Company performed a query (grep) in the DSAR results for all outgoing Telemetry Data in the intercepted network traffic, and did not find any match. It is plausible that Microsoft only provides access to server-side generated diagnostic data via the DSAR tool, and not to any of the received telemetry data from the end user device. It follows that the DSAR is incomplete, as Microsoft does not provide any access to the Telemetry Data that are clearly being sent to Microsoft in the outgoing data traffic. Microsoft has offered several reasons for this omission to the Dutch government, explained in the assessment below.

Many types of events contain pseudonymised identifiers for the user and for the tenant, such as "UserId": "b2814ab7-0cdb-4b7c-98fe-26deea388bb3", as shown in <u>Figure 48</u> below. None of the events contain the names of tested malware, or malicious mails and websites.

Figure 48: Example of telemetry event with pseudonymised identifiers

```
{
    "time": "",
    "correlationId": "",
    "properties": {
        "CountryCode": "NL",
        "Lcid": "EN-GB",
        "PreferredLanguage": "en-GB",
        "SnapshotDate": "2022-04-01T00:00:00.0000000",
        "TenantId": "bd9a989d-e990-4e6e-9566-5a8b29c3b6ff",
        "UsageLocation": "NL",
        "UserID": "b2814ab7-0cdb-4b7c-98fe-26deea388bb3",
        "WindowsLiveNetId": "1003200138B0D6A3",
        "WindowsLiveNetIdLong": "1153801119155148451"
    }
},
```

Answering the DSAR took considerably longer than earlier requests filed by Privacy Company with Microsoft: previously, in the same minimalistic test environment, Microsoft was able to complete the output within a couple of days. As shown in <u>Figure 49</u> below, Microsoft tells requesters it usually is able to comply within a few days, but warns it may take longer, without specifying the reasons.

$\leftrightarrow \rightarrow C$	A https://portal.azure.com/#blade/Microsoft_Azure_Resources/UserPrivacyMenuBlade/ManageUserRequests					
Microsoft Azure		₽ Search resources, services, and docs	(G+/)			
Home > User privacy						
🤱 User privacy	Manage User Requests					
	Add export request + Add delete request is Go to Azure AD to delete user O Refresh					
Overview Manage User Requests	<ul> <li>Data export or deletion request times can vary depending on a number</li> </ul>	er of factors. In most cases it should comple	te in a day or two, b.	it can take up to 30 d	ays.	
		Requests summary				
		Pending	Complete	Total		
	Data request type Data Subject Rights (DSR) Request	0 😑	10	1		

Figure 49: Microsoft information about time to answer DSARs

## 10.3 Assessment

Microsoft's assertion in 2020 that the Device ID was not personal data, was incorrect. Devices protected by organisations with an Enterprise or Education license are generally only used by a single user. In the test tenant Privacy Company could guarantee this single-user usage. This means the Device ID can be related to an individual and all data connected to the Device ID have to be qualified as personal data. In reply to this report, in April 2023 Microsoft has confirmed this reasoning, and will soon publish an overview of identifiers collected in Defender logs.

As explained in the Technical Findings, Microsoft's DSAR results for the Diagnostic Data are a hodgepodge of files with varying structures. This does not comply with the Art. 12 GDPR requirements to provide the requested information in an *intelligible and easily accessible form*.

Microsoft clearly has processes in place to replace directly identifying personal data such as email addresses and confidential data such as document names with generic replacements, or specific pseudonymous identifiers. These processes are not yet flawless: as shown in Figure 47 the events may still contain some direct identifiers. This is not in line with Microsoft's assurance that the Diagnostic Data should not contain any identifiable user data, different from the functional data that are necessary to provide the contracted (cloud) services, and apart from a specific exception for OneDrive.<sup>72</sup>

Events in the second category of 'other' data only appear to contain pseudonymised identifiers. None of the DSAR files contain names of e-mails or documents with malware or URLs of malicious websites,

At first sight, it appears Microsoft does not provide access to any of the intercepted Telemetry Data, only to the server-side generated data. This conclusion is based on the fact that none of the outgoing telemetry events intercepted from the outgoing data traffic appear in the DSAR results.

It is possible that Microsoft applied a data minimisation procedure to the incoming telemetry events, and only gave back minimised contents (without the header) of the stored Telemetry Data. However, even if such a procedure were applied, the results do not comply with the requirements for Data Subject Access as defined in Article 12 (form and comprehensibility) and 15 (right to access) of the GDPR.

Microsoft explains that it routinely deletes the personal data that are not Customer Data at most within 180 days.<sup>73</sup> This includes all types of Diagnostic Data (telemetry and server-generated service logs). It is possible that some telemetry data were already deleted during the 30 days Microsoft took to provide the requested access.

In view of the very limited activities deployed in the test tenant, and the fact that only 3 users (1 admin and 2 end users) were configured, the period of 30 days to answer the request seems overly long. Moreover, this time period puts Microsoft's customers, the government organisations that are the data controllers, in an impossible position to answer data subject access requests in time. At most, the controller will have one or two hours left to provide the data subject with Microsoft's answers to stay within the primary GDPR deadline of 30 days. Of course the employer can communicate that an extension of this deadline is necessary, but there does not appear to be a legitimate reason for such an extension.

<sup>&</sup>lt;sup>72</sup> Microsoft letters of 8 and 27 June 2021, in reply to the second technical verification report on the core Office 365 Suite as mobile apps and as Office for the Web, and in reply to the findings of the first Cluster DPIA on Teams, OneDrive, SharePoint and the Azure AD on all platforms.

<sup>&</sup>lt;sup>73</sup> Microsoft, Data retention, deletion, and destruction in Microsoft 365, 17 November 2021, URL: <u>https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview</u>

The lack of access to the Telemetry Data runs afoul of Microsoft's public commitment to provide access to the Required Service Data, as quoted in <u>Figure 46</u> above. Such access is even more necessary for data subjects to exercise their rights now that Microsoft does not want to publish event-level information, nor provide access through a Data Viewer Tool, because this would "*include confidential security or other proprietary information about the operation of our services, where publication of such data could put our services, and thus our customers and Microsoft, at risk.*"

Apparently, with this argument, Microsoft claims that it can rely on an exception to the GDPR transparency rights in Art. 23 (1) sub i of the GDPR, as translated for controllers in the Netherlands in Art. 41(1) sub i of the UAVG. This provision allows data controllers not to provide information about, or access to personal data as far as this is necessary and proportionate to safeguard the rights and freedoms of others. In order to successfully claim that the right or freedom of another, such as Microsoft itself, prevails over the rights of the requesting data subject, Microsoft must evidence what important interests necessitate the exception and why these outweigh the rights of the requesting data subject.<sup>74</sup> However, Microsoft does not provide any public information about this categorical refusal.

Generally speaking, nor controllers nor data processors can successfully claim company confidentiality to refrain from disclosing what categories of personal data they process. As the EDPB notes in its Guidelines on the restrictions under Art. 23 GDPR<sup>75</sup> restrictions on the data subjects rights can only be exceptional, not structural, and a strict necessity and proportionality test is required:

"The case law of the CJEU applies a strict necessity test for any limitations on the exercise of the rights to personal data protection and respect for private life with regard to the processing of personal data: 'derogations and limitations in relation to the protection of personal data (..) must apply only insofar as is strictly necessary'.<sup>76</sup> The ECtHR applies a test of strict necessity depending on the context and all circumstances at hand, such as with regard to secret surveillance measures."<sup>77</sup>

In sum, in its role as data processor, Microsoft is obliged to assist its Enterprise customers that are the data controllers with any requests for access ex Art. 15 GDPR. Microsoft has created two dedicated tools for admins to help them answer such requests. One tool to retrieve Content Data, and a second tool to retrieve Diagnostic Data relating to a specific user. However, the results of this second tool do not comply with Microsoft's processor commitments in multiple ways. First of all, the format and structuring of the data are not uniform or intelligible, while (second) the contents structurally omit many categories personal data, are stripped of context and cannot

<sup>74</sup> See for example the ruling from the administrative court Utrecht from June 2020, par. 19, URL: <u>https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2020:2222</u>

<sup>75</sup> EDPB, Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 1.0, Adopted on 15 December 2020, URL: <u>https://edpb.europa.eu/sites/default/files/consultation/</u> <u>edpb\_guidelines\_202010\_article23\_en.pdf</u>

<sup>76</sup> The EDPB refers to CJEU, judgment of 16 December 2008, case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, ECLI:EU:C:2008:727, paragraph 56.

<sup>&</sup>lt;sup>77</sup> The EDPB refers to ECtHR, Szabo and Vissy v. Hungary, 12 January 2016, paragraph 73.

be compared to any telemetry events and third, Microsoft does not provide a specific explanation why some data are not provided due to a legal exception, such as infringement on the rights of Microsoft.

## 10.4 Remedies

In order to remedy these deviations, <u>Microsoft is advised to take the following 3</u> remedies.

- 1. Speed up the process of providing access to the Diagnostic Data (taking less time to answer)
- 2. Stop collecting identifying data via the browser telemetry data or provide access to all personal data processed by Defender in a concise, transparent, intelligible and easily accessible form
- 3. If Microsoft wants to rely on an exception to the access rights from Art. 23 (1) under i of the GDPR jo. Art. 41(1) sub i of the UAVG, Microsoft should explain in detail why restrictions of the right to access some events would be necessary to safeguard the protection of the data subject or the rights and freedoms of others, including Microsoft itself.

# 11. Transfer risks

This section answers the final (ninth) verification question:

Are there high risks resulting from the transfer of personal data to the USA or other third countries?

## 11.1 Facts

Microsoft is moving data processing to the EU, with its EU Data Boundary program.<sup>78</sup> Currently, EU customers can already choose to have most Content Data processed, and service generated server logs generated in the EU. At the end of 2023, all Telemetry Data should also exclusively be processed in the EU. By the end of 2024, EU Enterprise and Education customers can choose to have all support tickets dealt with by exclusively EU based support employees.

In reply to questions from SLM Rijk, Microsoft explained that there are some exceptions to the EU Data boundary: some Content Data with pseudonymised identifiers from Defender for Endpoint, and a generic exception of all pseudonymised logs.

"All Customer Data for Defender services is stored at rest in the EU except for a small amount of customer content for Microsoft Defender for Endpoint that is transferred to the United States for the limited purpose of improving the Defender services' ability to protect from threats. The content transferred is data such as command lines, filenames, file paths, and URLs. Prior to transfer, the content is processed to pseudonymize potential identifiers.

*In addition, pseudonymized personal data is also transferred to the United States to be used for improving product protection. All data transferred to the* 

<sup>&</sup>lt;sup>78</sup>: Microsoft, Continuing Data Transfers that apply to all EU Data Boundary services, 27 April 2023, URL: <u>https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services</u>.

United States is maintained in protected data stores with controls to ensure that it is only processed for permitted purposes."<sup>79</sup>

Even though Microsoft already generates the service generated server logs in the EU, Microsoft currently systematically transfers aggregated logs to the USA.

"Microsoft online services create system-generated logs as part of the regular operation of the service. Currently all system-generated logs are aggregated globally in the United States. These system-generated logs may contain pseudonymized personal data. Examples of system-generated logs that may contain pseudonymized personal data include:

- Product and service usage data such as user activity logs
- Data specifically generated by interaction of users with other systems

Microsoft has explained it will stop processing these aggregated logs in the USA upon completion of the EU Data Boundary.

#### Microsoft writes:

"This EU Data Boundary documentation reflects the current state of the EU Data Boundary as of the date of publication. As noted in many cases in this article, we are continuing to deploy more services, service capabilities, and associated data within the EU Data Boundary and will update this documentation accordingly and note the last updated date."

Pseudonymization, as defined in Article 4(5) of the GDPR, is the processing of personal data so that it can no longer be attributed to a specific data subject without using additional information. In other words, it takes personally identifiable information within a data record and replaces it with one or more artificial identifiers, or pseudonyms, thus protecting the data subject's identity.

Microsoft has explained to SLM Rijk that it requires all personal data in systemgenerated logs to be pseudonymized. Microsoft uses various techniques to pseudonymize personal data in system-generated logs, including encryption, masking, tokenization and data blurring. Regardless of the specific method of pseudonymization, this protects user privacy by enabling authorized Microsoft personnel to use system logs containing only personal data that has undergone the security step of pseudonymization.

SLM Rijk has asked Microsoft to clarify what it meant with pseudonymisation of Content Data, as Diagnostic Data may also contain Content Data and personal data in file and folder names. Microsoft explained that it considers all data collected by Defender as Customer Content Data, even though the data Defender collects typically look like a form of system data.<sup>80</sup>

<sup>&</sup>lt;sup>79</sup> Idem.

<sup>&</sup>lt;sup>80</sup> E-mail Microsoft to SLM Rijk, 14 April 2023.

# 11.2 Technical findings

There are no technical findings.

## 11.3 Assessment

There is a (theoretical) risk that Microsoft is compelled to hand over personal data obtained from customers for this security purpose to law enforcement authorities or security agencies and secret services. This transfer risk has been thoroughly analysed in the Data Transfer Impact Assessment (DTIA) accompanying the 2022 public DPIA on Teams, OneDrive and SharePoint. The DTIA concludes that the chance is very slim that Microsoft is compelled to disclose personal data from EU public sector customers. Though Microsoft cannot disclose if it has **received** any specific legal demands subject to a secrecy obligation, it can explain that it has never **disclosed** personal data. Microsoft publicly explains:

"Microsoft does **not provide**, and has never **provided**, EU public sector customer's personal data to any government." This 'never' explicitly includes secret services, even though Microsoft is prohibited from disclosing if it has received orders under secrecy obligation.<sup>81</sup>

As a result of the EU Data Boundary, Content Data from EU customers are already exclusively processed in the EU, as well as the system generated server logs. By the end of 2023, Microsoft also expects to process all telemetry data and the aggregated data from the server logs exclusively in the EU.

If US authorities want access to these data, they can invoke the US Cloud Act. This act offers meaningful options for Microsoft to resist disclosure. If the names of specific employees or system administrators are too sensitive to transfer, the organisation can pseudonymise those names with identity federation.

By the end of 2024, all support tickets from EU Enterprise and Education customers will also exclusively be dealt with by agents based in the EU. If customers want to minimise the risk of unauthorised access to the contents of these support tickets in third countries, they can instruct staff never to include personal data in support tickets (except for the name of the person filing the ticket).

Additionally, Microsoft pseudonymises the personal data it processes for security purposes, provides legal guarantees of contesting each order, has a proven track record of such resistance, pledges to pay the customer damages if such compelled disclosure occurs and publishes detailed transparency reports twice per year.

Finally, it is likely that the European Commission will adopt a new (third) adequacy decision about the data protection rules in the USA in the summer of 2023.

On 25 March 2022, President Joe Biden and European Commission President Ursula von der Leyen signed an agreement 'in principle' to work out legal measures to ensure adequate protection of the data from the commercial sector in the USA. <sup>82</sup> On 7 October 2022, Biden signed a new Executive Order implementing this agreement with new binding safeguards for the data collection by US intelligence agencies, and

<sup>&</sup>lt;sup>81</sup> Microsoft, Compliance with EU transfer requirements for personal data in the Microsoft cloud, November 2021, URL: <u>https://go.microsoft.com/fwlink/p/?LinkID=2184913</u>.

<sup>&</sup>lt;sup>82</sup> European Commission press release, European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework, 25 March 2022, URL: <u>https://ec.europa.eu/commission/presscorner/detail/en/IP\_22\_2087</u>

introducing a new redress procedure.<sup>83</sup> Following this EOP, the European Commission prepared a new draft adequacy decision.<sup>84</sup>

The Commission has asked the EDPB for an Opinion. The EDPB has issued its Opinion in February 2023. The EDPB notes the substantial improvements offered by EOP, but expresses concerns, asks for clarifications from the Commission and calls on the Commission to monitor the implementation in future joint reviews.<sup>85</sup> The LIBE committee of the European Parliament has taken a critical stance.<sup>86</sup> After the non-binding vote in the plenary EP, the ministers of the Member States are invited to agree (the Council). A possible new adequacy decision is not expected before July 2023.

If the EC succeeds in adopting a new adequacy decision, Microsoft will not have to sign up or certify for adequacy. The adequacy decision will apply to all transfers to the USA, also when based on SCCs and BCR.<sup>87</sup> Max Schrems immediately announced that he would likely challenge the arrangement once again at the European Court of Justice: "*noyb expects to be able to get any new agreement that does not meet the requirements of EU law back to the CJEU within a matter of months e.g. via civil litigation and preliminary injunctions. The CJEU may even take preliminary action if a deal is clearly violating previous judgements."<sup>88</sup>* 

**In sum**, based on the extremely small chance that the risks of unauthorised access to the personal data materialise at Microsoft and the upcoming new adequacy decision for the USA, the risk of undue access to these pseudonymised security data can be qualified as a low data protection risk.

#### 11.4 Remedies

Microsoft is advised to clarify the documentation about the EU Data Boundary. It must be clear what data will be transferred to the USA and possibly other third countries after completion of the EU Data Boundary.

<sup>&</sup>lt;sup>83</sup> Executive Order of the President, Enhancing Safeguards for United States Signals Intelligence Activities, URL: <u>https://www.whitehouse.gov/briefing-</u>

 $<sup>\</sup>frac{room/presidentialactions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signalsintelligence-activities/$ 

<sup>&</sup>lt;sup>84</sup> Press release European Commission, Commercial sector: launch of the adoption procedure for a draft adequacy decision on the EU-U.S. Data Privacy Framework, 12 December 2022, <u>https://commission.europa.eu/law/law-topic/data-protection/international-dimension-dataprotection/eu-us-data-transfers\_en</u>.

<sup>&</sup>lt;sup>85</sup> EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, 28 February 2023, URL: <u>https://edpb.europa.eu/system/files/2023-02/edpb\_opinion52023\_eu-us\_dpf\_en.pdf</u>.

<sup>&</sup>lt;sup>86</sup> LIBE list of proposed amendments on draft report, 9 March 2023, URL: <u>https://www.europarl.europa.eu/doceo/document/LIBE-AM-745289\_EN.pdf</u>.

<sup>&</sup>lt;sup>87</sup> Stated by Commissioner Didier Reynders in reply to questions from the European

Parliament, 24 June 2022, URL: <u>https://www.europarl.europa.eu/doceo/document/E-9-2022-</u>001307-ASW EN.html.

<sup>&</sup>lt;sup>88</sup> Noyb, "Privacy Shield 2.0"? - First Reaction by Max Schrems, 25 March 2022, URL: <u>https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems</u>

Organisations are advised to consider the use of pseudonymous accounts for specific employees working with for example secret information, and use pseudonyms for the system administrators.