DPIA *on-premise* Microsoft 365 Dynamics

Data protection impact assessment on the processing of personal data with *on-premise* Microsoft 365 Dynamics

Version 1.2

Date	31 August 2023
Status	Public

Colophon

DPIA by	**Ministry of Justice and Security** **Strategic Vendor Management Microsoft, Google and Amazon Web Services** (SLM Rijk) Turfmarkt 147 2511 DP Den Haag PO Box 20301 2500 EH The Hague www.rijksoverheid.nl/jenv
Contact	E slmmicrosoft@minjenv.nl T 070 370 79 11
Project Name	**DPIA report** on *on-premise* Dynamics 365
Authors	**Privacy Company** Sjoera Nas Floor Terra based on a report from Lennard Huizinga Senior Advisors www.privacycompany.eu

Change log

Version	Date	Summary of input
0.9	3 November 2022	First draft umbrella report
1.0	21 July 2023	Input Microsoft processed in track changes
1.1	21 July 2023	Clean version
1.2	31 August 2023	New public version after input Microsoft with policy to block telemetry data

Summary

This report, commissioned by SLM Microsoft, Google and Amazon Web Services Rijk (SLM Rijk), contains a Data Protection Impact Assessment (DPIA) on the use of the *on-premise* installation of Microsoft Dynamics 365 software for customer relationship management, in combination with Microsoft's Azure Active Directory cloud service. Dynamics helps organise external relations. With the marketing module Dynamics can be used to send newsletters and mailings with invitations for events with the marketing module.

Outcome: no more high data protection risks
The outcome of this DPIA is that there are no more known high risks related to the use of the investigated *on-premise* Microsoft Dynamics 365 software for customer relationship management.

Initially this DPIA identified five high data protection risks for data subjects. Microsoft responded by taking technical measures and providing guidance on technical measures admins can take to mitigate risks. Microsoft has also provided missing information about the nature of the data processing. Finally, Microsoft benefits from the new adequacy decision from the European Commission for the USA with regard to the transfer to the USA of Account Data via the Azure Active Directory (Azure AD, new name: Entra). In the test setup this cloud service was used to enable employees and admins to log-in to the database.

The original DPIA was performed for a specific government organisation, and identified some specific risks related to the setup of the test environment. These specific risks have been removed from this umbrella DPIA, to make this report more useful for all government organisations that wish to use this software.

The five high risks were due to the following circumstances:

1. The incomplete removal of personal data. When an employee deletes a contact from the database, for example because an individual has withdrawn consent, or because the retention period has expired, the Audit table continues to store the removed Content Data. The Content Data may include sensitive or special categories of data, relating to for example special needs or dietary allergies. In reply to this DPIA, Microsoft has pointed to guidance for admins how to delete specific Content Data from the Audit tables, and how to remove names of former employees without compromising the integrity of the audit log.
2. Preventing data subjects from fully exercising their rights. Microsoft did not reply to a Data Subject Access Request. Microsoft explained that government organisations that use the *on-premise* Dynamics software have full access to all available personal data, and can hence answer all data subject access requests themselves. In the test set-up there was no portal with Do It Yourself access for external data subjects.
3. Inclusion of a tracking pixel in newsletters. By default, Microsoft includes a tracking pixel in the mailings that are sent through the marketing module. With this tracking pixel, government organisations can see what individual recipients opened the mailing and when they did. Based on the ePrivacy Directive, as implemented in the Dutch Telecommunications Act, the use of such a tracking pixel requires prior informed consent from the recipients. During this DPIA, Microsoft added a technical option for admins to turn off the tracking pixel for all or for individual recipients.

4. Lack of transparency about the Diagnostic Data processed by the Dynamics software. In reply to this finding, Microsoft has explained that some server Telemetry Data, collected from versions of the *on-premise* software installed before 2018, is outdated, and is no longer used. Microsoft has provided a policy that admins should use to disable this data traffic.
5. The transfer of Account Data from admins and employees from the Azure AD to the USA, and to the third countries Singapore and Australia through the use of a subprocessor for captchas. Microsoft has explained that Enterprise and Education customers are never shown captchas, and hence, there is no risk for transfer of personal data to this subprocessor.

The original risks, with the remaining recommended mitigating measures for government organisations and for Microsoft, are listed in the table below:

Risk no.	**Risk**	**Measures government organisation**	**Measures Microsoft**
1.	Possible unlawful continued processing of personal data (including sensitive and special categories of data) in Audit tables.	Review the lawfulness of including sensitive and special categories of data in the Audit tables, or follow the guidance from Microsoft to exclude these data from the Audit tables.	- no measures necessary, guidance is available at https://learn.microsoft.com/en-us/dynamics365/customerengagement/*on-premise*s/admin/audit-data-user-activity?view=op-9-1#enable-or-disable-entities-and-fields-for-auditing.
2.	Use of tracking pixels in newsletters without consent.	Update the software to benefit from the new option, and disable use of tracking pixels in newsletters sent with the marketing module.	- no measures necessary, Microsoft enables admins to disable the tracking pixel via https://learn.microsoft.com/en-us/dynamics365/marketing/privacy-use-features .
3.	Inability to exercise data subject rights.	It is possible to use Dynamics as *on-premise* software and not use cloud services such as the Azure AD.	- no measures necessary, admins have access to all Content Data and logs.

		If a government organisation uses the Dynamics cloud services, they can obtain access to Content Data via the Security & Compliance center, and the Azure export tool for system-generated logs.	Information about export of Content and Diagnostic Data in the cloud services is available at https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-data-subject-requests#data-subject-request-admin-tools.
4.	Lack of legal ground for collection of legacy server Telemetry Data (Microsoft controller).	Block sending of legacy server Telemetry Data (possibly with the help of an implementation partner).	- no extra measures necessary, Microsoft no longer collects these data in newer server versions.
5.	Transfer of Account Data to Singapore, Australia and the USA	Prevent the 3 situations in which the Azure AD data are transferred to the USA.	Complete the EU Data Boundary for the Azure AD, regardless of the new adequacy decision.
		Use pseudonyms if the identity of specific employees should remain secret. If that is insufficient, do not use the Azure AD cloud for authentication, only the *on premise* AD.	No measures necessary with regard to Arkose Labs Inc, as this subprocessor is not used for Enterprise customers

Conclusion
Microsoft has taken adequate technical measures or provided relevant information to mitigate the initially identified 5 high risks. If the government organisations apply the recommended risk mitigating measures in this DPIA, there are no known high or low data protection risks.

Microsoft can take one more measure to solve the low risk of transfer of personal data to the USA, if organisations use the Azure AD cloud service for authentication, to exclusively process the Azure AD data in the EU Boundary.

Contents

Introduction

Microsoft Dynamics 365 is a customer relationship management system that helps organisations to manage their relations. This report, commissioned by the strategic vendor management office of the Dutch government for Microsoft, Google and Amazon Web Services (SLM Rijk), housed at the Ministry of Justice and Security, is a Data Protection Impact Assessment (DPIA) about the *on-premise* server of Dynamics 365.

The technical inspection of the data processing for this DPIA was performed on a test setup for a specific Dutch government organisation as a basis for fact finding

DPIA

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

A DPIA used to be called PIA, *privacy impact assessment*. According to the GDPR a DPIA assesses the risks for the rights and freedoms of individuals. Data subjects have a fundamental right to protection of their personal data and some other fundamental freedoms that can be affected by the processing of personal data, such as for example freedom of expression.

The right to data protection is therefore broader than the right to privacy. Consideration 4 of the GDPR explains:

> "*This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity*".

This DPIA follows the structure of the DPIA Model mandatory for all Dutch government organisations.[1]

Umbrella DPIA versus individual DPIAs

Pursuant to article 35 of the GDPR, a DPIA is mandatory if an intended data processing constitutes a high risk for the data subjects whose personal data are being processed. The Dutch Data Protection Authority (Dutch DPA) has published a list of 17 types of processing for which a DPIA is always mandatory in the Netherlands.[2] If a processing

[1] Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) (September 2017). For an explanation and examples (in Dutch) see: https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia. The model will be replaced by version 2.0, not yet published. See: https://ib-p.nl/2022/02/model-dpia-rijksdienst-2-0-whats-new/.

[2] Dutch DPA, list of processings for which a DPIA is required, in Dutch only, Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een

is not included in this list, an organization must itself assess whether the data processing is likely to present a high risk.

The European national supervisory authorities (hereinafter referred to as the Data Protection Authorities or DPAs), united in the European Data Protection Board (EDPB) have also published a list of 9 criteria.[3] As a rule of thumb if a data processing meets two of these criteria a DPIA is required.

In GDPR terms SLM Rijk **is not the data controller** for the processing of personal data via the use of the *on-premise* Dynamics 365. The data controller is the individual government organisation that decides to use this software. However, as central negotiator for many cloud services, SLM Rijk has a moral responsibility to assess the data protection risks for the employees and negotiate for a framework contract that complies with the GDPR. Therefore, SLM Rijk commissions umbrella DPIAs to assist the government organisations to select a privacy-compliant deployment, and conduct their own DPIAs where necessary. Only the organisations themselves can assess the specific data protection risks, related to the technical privacy settings, nature and volume of the personal data they process and vulnerability of the data subjects.

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

Dutch government organisations frequently use Microsoft software, including Dynamics as software or as service. Because the data processing takes place on a large scale, the data processing involves data about (marketing) communication (be it content or metadata) and involves data that can be used to track the activities of employees, it is mandatory for organisations in the Netherlands to conduct a DPIA based on the criteria published by the Dutch DPA.[4]

Scope of this DPIA

The scope of this DPIA is limited to the personal data processed in and about the use of the *on-premise* Dynamics 365 server, with access through a browser on a Windows 10 desktop.

The term *on-premise* has different meanings. It can be used if an organisation hosts the software on a server on its own physical premises, but Microsoft also uses this term if an organisation implements Dynamics 365 on a server of its own choosing, including servers from hosting providers. This option was tested for this DPIA.

In the test setup Azure Active Directory was used for identification. Therefore, this report also addresses transfer risks.

---

gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf.

[3] The EDPB has adopted the WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248rev.01, 13 October 2017, URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[4] Dutch DPA, list of processings for which a DPIA is required, in Dutch only, Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf

Out of scope
The following types of data processing are out of scope of this DPIA:

- Microsoft Dynamics 365 as a cloud service and related Microsoft server-generated system logs.
- Support Data shared with Microsoft (through a separate support plan or Professional Services contract).
- Dynamics 365 Customer Insights.
- Dynamics 365 Fraud Protection.
- The effectivity of the new privacy option for admins to disable the tracking pixel in newsletters sent through Dynamics.
- Optional monitoring features that must be specifically switched on or that require the customer to install add-ons to *on-premise* Dynamics 365.

Technical research
Privacy Company has performed a black-box assessment of the local processing of personal data in the test setup . In contrast with other DPIAs, Privacy Company was not able to intercept any traffic and inspect the resulting logfiles itself, but had to rely on the information provided by the Dynamics administrators of the test setup.

In order to collect information about the data processing through the software, Privacy Company asked an employee of the specific Dutch government organisation to run several test scenarios. The scenarios were written to imitate the average activities of a government administrator to add or delete personal contact data from the database. The test scenarios were executed on a desktop computer with Windows 10 Enterprise, in the default work configuration at the specific Dutch government organisation with the *on-premise* Dynamics 365 server, with an Edge browser. The test scenarios were executed twice (in August and October 2019), to take changes of the configuration into account. The organisation provided access to the technical logfiles generated as a result of the execution of the test scenarios, filtered for data that were relevant for the specified User ID.

Privacy Company obtained access to some of Microsoft's Dynamics logs in February 2020, and access to the Audit tables in June 2020. Privacy Company was not able to test the effectivity of the new privacy option to disable the pixel in the newsletters.

In September 2020, Privacy Company conducted a further check on the use of cookies on the log-in page. This test appeared to show that Microsoft collected Telemetry Data through the browser. In July 2023 Microsoft explained that these Telemetry Data were generated by other Microsoft cloud services, such as SharePoint online and Exchange Online. Microsoft also provided information about the Telemetry Data sent from the *on-premise* server. In August 2023 Microsoft explained that it does not use subprocessors in third countries when the EU Data Boundary applies to services. Microsoft also provided a policy to block the obsolete Telemetry Data from pre-2018 installs of the *on-premise* server software, and confirmed the analysis of Privacy Company about the unclear role of Microsoft as processor or controller for the software.

Timeline of this DPIA
This data protection impact assessment was carried out by Privacy Company as commissioned by SLM Rijk between April 2019 and August 2023. It builds on previous DPIAs on Microsoft products and services commissioned by SLM Rijk, and takes as a

starting point for the legal analysis the improved framework contract of the Dutch government with Microsoft.

The process of compiling and writing this DPIA was slow. In August and October 2019, test scenarios were executed on the test implementation at the specific Dutch government organisation and a data subject access request was filed with Microsoft. In May 2020 it became apparent that the external supplier had access to more log files and Audit tables than previously discovered. These were provided to Privacy Company in June 2020, resulting in a draft version of this report in July 2021.

Over the course of Q3 2020 additional data processings surfaced after additional inquiries were made. The processings were analysed and recorded in a final report in February 2021.

At the request of SLM Microsoft Rijk, this report was transformed in an umbrella DPIA and Microsoft was asked for feedback. In July and August 2023 Microsoft provided essential new information, and this report was rewritten accordingly.

Outline
This Data Protection Impact Assessment assesses the use of *on-premise* Microsoft Dynamics by Dutch government organisations for contact relationship management purposes, including the use of the marketing module to send newsletters.

The Dutch government DPIA-model uses a structure of four main divisions, which are reflected here as "parts".

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

Part A explains the tested *on-premise* Dynamics 365 solution. This part starts with a description of the way the data are collected and describes the categories of personal data and data subjects that may be included in the processing; the purposes of the data processing; the different roles of the parties involved; the different interests related to this processing; the locations where the data are stored, and the retention periods. Part A also lists the relevant legal documents that govern the processing of data resulting from the use of *on-premise* Dynamics 365.

Part B provides an assessment of the lawfulness of the data processing through the *on-premise* Dynamics 365. This analysis starts with an overview of the extent to which the GDPR and the ePrivacy Directive apply to these processings, in relation to the legal qualification of the role of Microsoft as provider of the software and services. Subsequently, part B provides an assessment of the conformity with the key principles of data processing, including transparency, data minimisation, purpose limitation, and the legal ground for the processing, as well as the necessity and proportionality of the processing. In this section the legitimacy of any transfers of personal data to countries outside of the (European Economic Area (EEA) is separately addressed, as well as an analysis how Microsoft treats requests from data subjects to exercise their rights.

Part C assesses the risks to the rights and freedoms of the data subjects caused by the processing activities identified resulting from the use of the *on-premise* Dynamics 365 in Part A of this DPIA. It names specific risks that derive from these processings and aims to specifically determine both the likelihood that these risks may occur, and

the severity of the impact on the rights and freedoms of the data subjects if the risks occur.

Finally, **Part D** contains the specific measures that can be taken by either Microsoft or the individual government organisations to mitigate high or low risks. These measures might either reduce the chance the risks occur, or the impact they might have, or both.

Part A. Description of the Data Processing

This first part of the DPIA provides a description of the data processing through a specific *on-premise* installation of Microsoft 365 Dynamics.

1. The Processing of Personal Data

1.1 Data processing by Dynamics 365

Microsoft Dynamics 365 was developed by Microsoft as a group brand of Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) applications.

Microsoft Dynamics 365 offers a wide range of solutions to manage data for Sales, Customer Service, Field Service, Talent, Finance and Operations, Retail, Project Service Automation, Marketing, Artificial Intelligence, Mixed Reality, and Business Central.[5] This report is focussed on the platform to manage customer relationships for first contact, purchase, and post sales. This was called Microsoft Dynamics CRM until the end of 2016. Microsoft now calls this platform *Dynamics 365 Customer Engagement (on-premises)*.[6] It is highly customizable, and includes a marketing module to send newsletters.[7]

Microsoft Dynamics 365 can be used in combination with other Microsoft programs and services, such as Sharepoint Online, Yammer, Office 365, Azure, and Exchange Online/Outlook. To enable this combination, Dynamics is based on the so-called "Common Data Model" (CDM).[8] This means that the data are entered and maintained in a standardised format, enabling the use of data across many different applications. Additionally, each app may have its own data and schemas, depending on its functionalities.[9]

There are three main options in the deployment of Microsoft Dynamics 365: Customers can choose between

1. deploying the software in Microsoft's cloud (resulting in the deployment as a Software-as-a-Service (SaaS) solution),
2. on a partner-hosted cloud chosen by the customer, or
3. on the customer's physical premises.[10]

A hybrid of *on-premise* and server-hosted deployment is also possible.

---

[5] Microsoft Dynamics Homepage, Applications, URL: https://dynamics.microsoft.com/en-us/.

[6] Microsoft, Microsoft Dynamics 365 Customer Engagement (on-premises) Help, version 9.x , 9 January 2023, URL: https://learn.microsoft.com/en-us/dynamics365/customerengagement/on-premises/overview?view=op-9-1

[7] Microsoft, What is CRM? undated, URL: https://dynamics.microsoft.com/en-us/crm/what-is-crm/.

[8] Microsoft, What is the Common Data Model?, undated. URL: https://dynamics.microsoft.com/en-us/microsoft-power-platform/common-data-model/.

[9] Microsoft, The Common Data Model, 7 April 2022, URL: https://docs.microsoft.com/en-us/common-data-model/ .

[10] Microsoft Dynamics 365 Licensing Guide, June 2023 p. 1, URL: https://download.microsoft.com/download/9/6/7/96706B15-1CBE-47B7-AB9E-6BC31A377BBB/Dynamics%20365%20Licensing%20Guide%20-%20June%202023.pdf . This guide does not apply to *on-premise*s solutions.

This DPIA examines the risks to the rights and freedoms of data subjects of the use of the second option: an *on-premise* installation of Microsoft Dynamics 365 in a partner-hosted cloud, in combination with the (optional) Microsoft's Azure Active Directory cloud service.

In the test set-up, the data processed through *on-premise* Dynamics 365 were collected during four processes:

1. Entry of contact data by employees in the database.
2. Self-entry of sensitive data by visitors through a website, such as dietary requirements.
3. Generation by Microsoft of diagnostic data as a result of the use of the server software.
4. Generation by Microsoft of cookie and security logs as a result of the use of the Azure AD.

In the test setup, the government organisation used the server software for two main purposes of the data processing:

1. Relationship management: Entry, updating and manual deletion of contact information about relations of the government organisation;
2. Sending mailings: Selection of data subjects and inviting them to events.

The specific purposes are elaborated in Section 4.1.

1.2 Three categories of personal data

This report addresses the data protection risks of the processing of three kinds of personal data: Content Data, Account Data and Diagnostic Data. This DPIA does not assess the processing of Support Data, or the data processed by Microsoft as controller for its own public website. The processing of these data has already been addressed in previous DPIAs for SLM Rijk.[11]

1. **Content Data** are the personal data actively stored in the database. Microsoft calls these data Customer Data.
2. **Account Data** are the credentials used by employees to log-in to the *on-premise* server, in this case, Microsoft's Azure Active Directory.
3. **Diagnostic Data** are all data generated or collected by the *on-premise* software and by Microsoft as cloud service provider about the use of its server and services. Diagnostic Data include both Telemetry Data and service generated server logs (also called system generated logs), as well as cookie data collected as a result of online authentication with the Azure AD.

Telemetry Data are data generated on the end user device or browser, and sent in batches to Microsoft. Microsoft itself reserves the term 'Diagnostic Data' for Telemetry Data, and uses the term system generated logs for other Diagnostic Data

Server logs may be generated and stored in Microsoft's cloud (for example when the organisation uses the Azure Active Directory for employees to log-in to the *on-premise* server, or as log files (Audit tables) in the *on-premise* server.

Diagnostic Data include data about access to the web application via the browser after log-in by both employees and admins, but only to the extent that these data are

[11] These DPIAs and technical verification reports are published at www.slmmicrosoftrijk.nl

stored by the cloud provider and not merely transported. Diagnostic Data also include personal data relating to for example recipients of newsletters sent with the marketing module, and include so called Telemetry Data.

2. Personal Data and Data Subjects

The Dutch government DPIA model requires that this section provides a list of the kinds of personal data that will be processed, and per category of data subjects, what kind of personal data will be processed by the product or service for which the DPIA is conducted. To help readers that are not GDPR experts understand the data protection risks, this section explains in detail why the stored Diagnostic Data about the use of the *on-premise* Dynamics 365 software are personal data as defined in Article 4(1) GDPR.

The different kinds of data that Microsoft processes via *on-premise* Dynamics 365 will be described in more detail in Section 2.6 of this DPIA, with the technical findings.

2.1 Definition of personal data

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

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

In the Enterprise contract for Online Services, Microsoft uses the definition of Customer Data for all data that are actively provided by Customers. Customer Data do not include the metadata. However, based on the specific privacy amendment negotiated by the Dutch government, all personal data processed in Microsoft's Online Services (in this case the Azure AD), including all Diagnostic Data, are covered by the privacy guarantees and purpose limitation.

This umbrella DPIA can only indicate types of personal data and types of data subjects that may be involved in the processing, but cannot assess the specific risks of the actual data processing per organisation that uses or will use the *on-premise* Dynamics 365 software. The risks for data subjects strongly depend on the privacy choices and settings that each organisation makes, as well as on the nature of the work performed by their employees.

This DPIA provides a description of the possible kinds of Content Data that government organisations may process in the software, and the data subjects affected by the processing. See Section 2.3 below.

2.2 Categories of personal data in the Content Data

This section first provides a general description of the types of personal data that can be processed in Dynamics 365, distinguished in the impact of the processing on data subjects (confidential, sensitive and special categories of data). This section is followed by a specific description of the actual Content, Account and Diagnostic Data created and processed in the test setup.

2.2.1 Classified information

Dutch government employees will, depending on the capacity in which they work, often process Classified Information. The Dutch government defines 4 classes of

Classified Information, ranging from confidential within the ministry to extra secret state secret.[12]

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

If government organisations chose to use the Azure AD, or combine the use of *on-premise* Dynamics with cloud services such as SharePoint Online or OneDrive, they have to be aware that Microsoft may process classified information, including confidential file names and storage locations. A folder may for example have as name: "State Secret – negotiations with country/company X".

2.2.2 *Personal data of a sensitive nature*

Some types of personal data have to be processed with extra care, due to their sensitive nature. Examples of such sensitive data are financial data, communications traffic data and location data.

The sensitivity is related to the level of risk for the data subjects in case the confidentiality of the data are breached. Risks may vary from slight embarrassment if the employer notices from the log files that an employee has made several mistakes, to a chilling effect if the employer does not specifically exclude the use of the log files for performance assessments, to exposure of VIP data.

It is likely that many government employees process personal data of a sensitive nature about other data subjects on a daily basis. These Content Data are also stored in Audit tables, including data of a sensitive nature.

The *on-premise* Dynamics 365 implementation in the test set-up did not include any explicit use of sensitive categories of personal information (except for the dietary information, see below). However, it is plausible that some contact data are very sensitive, such as home addresses and phone numbers of politicians and high ranking government officials.

2.2.3 *Special categories of personal data*

Based on the GDPR, the processing of special categories of personal data is prohibited, unless one of the exceptions from the limitative list included in the GDPR applies.

According to Article 9 (1) GDPR, personal information falling into special categories of data are any:

> "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,*

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

data concerning health or data concerning a natural person's sex life or sexual orientation".

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

The *on-premise* Dynamics 365 does not by default process any special categories of personal data. Depending on the specific implementation by a customer, it is possible that special categories of personal data become part of the processing, and of the Audit tables. Microsoft has no direct influence over what data gets included in an implementation.

2.3 Categories of data subjects

The processing concerns two groups of data subjects: (i) the individuals whose data are entered into the application (the relations of the government organisation that wishes to use Dynamics, and possibly also data about their partners), and (ii) the employees of a government organisation that work with the application (including system administrators). With the term *employee* this report intends to describe a broad group of workers, regardless of their contracting situation as internal, temporary or external employees. Employees require system credentials and the way they use the system is recorded in log files. These data are stored for a defined period of time. This implies that the system could contain information about former employees if there were no possibility to delete individual credentials or log files.

2.4 Content Data

In the tested setup the following personal data were processed:

- Name
- Titles (hereditary, academic, etc).
- Gender
- Language
- Address
- Sensitive private contact details, including secret phone numbers, mail addresses and private addresses
- Email address
- Phone number
- Photo
- Social media accounts
- Employer (possible special category)
- Department
- Function
- Side activities and positions
- Contact preferences
- Lead status

- Notes*****
- Tasks
- Contact type
- Calendar-items
- Conversations
- Messages
- Diet*****
- Allergies*****
- Activities (historical transactions on the contact's information)
- Properties*****
- Related persons (link to another person's records)

***** These types of data might include special categories of personal data (see Section 12 of this report)

Every record in *on-premise* Dynamics 365 contains the following metadata:

- Date created
- Date updated
- Username
- Password
- Account setting

Customers are free to define the data type 'Properties'. This means this data type can contain anything that can help to create selections. These data persist after use and remain active until they are deliberately inactivated. After inactivation, they become invisible, but are not removed from the system until the contact is completely deleted.

In the Dynamics information schema for government system administrators Microsoft explains that the identifiers mentioned in **Error! Reference source not found.** below are always collected in server logs (*on-premise* or in the Microsoft cloud) when system administrators access *on-premise* Dynamics 365.[13]

[13] Microsoft, Microsoft Dataverse and model-driven apps activity logging, 7 March 2023, URL: https://docs.microsoft.com/en-us/power-platform/admin/enable-use-comprehensive-auditing

Figure 1: Microsoft table common identifiers collected about system admins

Base schema

Schemas define which fields are sent to the Microsoft Purview compliance portal. Some fields are common to all applications that send audit data to Microsoft Purview, while others are specific to customer engagement apps. The Base schema contains the common fields.

Field name	Type	Mandatory	Description
Date	Edm.Date	No	Date and time of when the log was generated in UTC
IP address	Edm.String	No	IP address of the user or corporate gateway
Id	Edm.Guid	No	Unique GUID for every row logged
Result Status	Edm.String	No	Status of the row logged. Success in most cases
Organization Id	Edm.Guid	Yes	Unique identifier of the organization from which the log was generated. You can find this ID under Dynamics Developer Resources.
ClientIP	Edm.String	No	IP Address of the user or corporate gateway
CorrelationId	Edm.Guid	No	A unique value used to associate related rows (e.g., when a large row is split)
CreationTime	Edm.Date	No	Date and time of when the log was generated in UTC
Operation	Edm.Date	No	Name of the message called in the SDK
UserKey	Edm.String	No	Unique Identifier of the User in AAD. AKA User PUID
UserType	Self.UserType	No	The Microsoft 365 audit type (Regular, System)
User	Edm.String	No	Primary email of the user

The tested implementation did include occasional processing of special categories of personal data. Often, relations are connected to the organisation they are affiliated with. The names of these organisations may reveal the political, religious or health background of those relations, for instance when the relation is a representative of a political party, a church, or a patient organisation. Trade union membership is also easily implied when the relation's employer is itself a trade union.

Additionally, the tested implementation of the *on-premise* Dynamics 365 included information about dietary needs and allergies. Dietary information can reveal information about health or religious affiliation. Allergy information is always informative of someone's health. Both are to be treated as special categories of personal data.

2.5 Account Data in the Azure AD

In the hybrid test set-up the Microsoft 365 Enterprise accounts, with the credentials and the related licenses, were registered in the Azure Active Directory (hereinafter: Azure AD). This is Microsoft's online cloud identity service. The Azure AD data globally include values like usernames, email addresses, IP addresses, and Azure AD tokens. After 1 October 2023, Microsoft will rename the Azure AD into Microsoft Entra.[14]

Use of the Azure AD cloud service is not necessary, organisations can also use an *on-premise* active directory to give people access to Dynamics. In the test set-up with the Azure AD employees had to visit the online Microsoft log-in page to authenticate themselves for access to the *on-premise* server via their browser. In the test setup there was no other access option (no installed apps on devices).

[14] Microsoft, New name for Azure Active Directory, 11 July 2023, URL: https://learn.microsoft.com/en-gb/azure/active-directory/fundamentals/new-name.

2.6 Diagnostic Data

Microsoft has programmed extensive logging capabilities into *on-premise* Dynamics 365.[15] If a customer uses Dynamics 365 as a cloud service, Microsoft can collect and process log files about user activities (actions performed on resources). However, in this DPIA, only an *on-premise* setup was tested. In this setup, the log files were created on the server controlled by the customer. Therefore, most of the log files described below are only accessible for the system administrators of the government organisation.

Microsoft describes the purpose of logging as follows:

> "*The Dynamics 365 Customer Engagement (on-premises) auditing feature logs changes that are made to customer records and user access so you can review the activity later. The auditing feature is designed to meet the auditing, compliance, security, and governance policies of many regulated enterprises.*
>
> *The audit logs help the Customer Engagement (on-premises) administrator answer questions such as:*
>
> - *Which user was accessing the system and when?*
> - *Who updated this field value on this record and when?*
> - *What was the previous field value before it was updated?*
> - *What actions has this user taken recently?*
> - *Who deleted this record?*
> - *What locale was used to make the update?*
> - *The following operations can be audited:*
> - *Create, update, deactivate, and delete operations on records.*
> - *Changes to the sharing privileges of a record.*
> - *The N:N association or disassociation of records.*
> - *Changes to security roles.*
> - *Audit changes at the entity, attribute, and organization level. For example, enabling audit on an entity.*
> - *Deletion of audit logs.*
> - *For changes made to entity fields that can be localized, such as the Product entity name or description fields, the locale ID (LCID) appears in the audit record.*
>
> *System administrators and customizers can start or stop auditing for an organization.*"[16]

The seven paragraphs below describe the different types of Diagnostic Data processed in the test setup.

---

[15] Microsoft, Manage Dataverse auditing, 20 April 2023, URL: https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/audit-data-user-activity.

[16] Microsoft, Audit data and user activity for security and compliance, 16 February 2022, URL: https://learn.microsoft.com/en-us/dynamics365/customerengagement/on-premises/admin/audit-data-user-activity?view=op-9-1.

1. Customer Audit tables with insights in the creation, reading, update and deletion of records;
2. Customer technical log files;
3. Customer logs about read rates of e-mails with the tracking pixel in newsletters;
4. Microsoft logs about the use of the Azure AD;
5. Microsoft Authentication data for browser access through cookies;
6. Microsoft Server Telemetry Data;
7. Unrelated Telemetry Data from Office 365 applications

2.6.1 *Customer Audit tables*

The *on-premise* Dynamics 365 stores every change to every content field by default, together with information about the time the change was entered into the system and by whom. These records are stored in so called Audit tables. These tables can be used to reconstruct and rectify errors. System administrators have the option to turn these audit logs on and off, but they were on during the time of the second run of the test scenarios.

Figure 2: Microsoft Dynamics User and support-related events[17]

User and support-related events

Event	Description
Create, read, update, delete (CRUD)	Logging all CRUD activities essential for understanding the impact of a problem and being compliant with data protection impact assessments (DPIA).
Multiple record view	Users of Dynamics view information in bulk, like grid views, Advanced Find search, etc. Critical customer content information is part of these views.
Export to Excel	Exporting data to Excel moves the data outside of the secure environment and is vulnerable to threats.
SDK calls via surround or custom apps	Actions taken via the core platform or surround apps calling into the SDK to perform an action needs to be logged.
All support CRUD activities	Microsoft support engineer activities on customer environment.
Admin activities	Admin activities on customer tenant.
Backend commands	Microsoft support engineer activities on customer tenant and environment.
Report Viewed	Logging when a report is viewed. Critical customer content information might be displayed on the report.
Report Viewer Export	Exporting a report to different formats moves the data outside of the secure environment and is vulnerable to threats.
Report Viewer Render Image	Logging multimedia assets that are shown when a report is displayed. They might contain critical customer information.

The Audit tables inspected by Privacy Company contain information about both the current and previous information about records that were changed. They also contain all deleted content, as configured in the test setup. The information about contacts contains the same categories of data as the rest of the application. The Audit tables also store personal data about employees of the government organisation: the time

[17] Microsoft, Microsoft Dataverse and model-driven apps activity logging, 7 March 2023, URL: https://docs.microsoft.com/en-us/power-platform/admin/enable-use-comprehensive-auditing

and date they interacted with the application, the records they accessed, as well as information about which changes they made to the data in *on-premise* Dynamics 365.

Collecting this type of information is often a vital part of securing the integrity of a system and to be able to detect weaknesses in the system.

As shown in **Error! Reference source not found.** below Microsoft provides a list of events with a description about the Audit tables.

When the testing was performed for this DPIA, Microsoft did not explicitly warn admins that the CRUD records (Create, Read, Update, Delete) contain the full contents of every changed or deleted record, including information about deleted fields. Inspection of the Audit tables showed that all data types mentioned earlier in this section, including the Content Data, were included. In other words, through the Audit tables the organisation continues to process deleted Content Data.

Figure 3: Anonymized sample of audit logs[18]

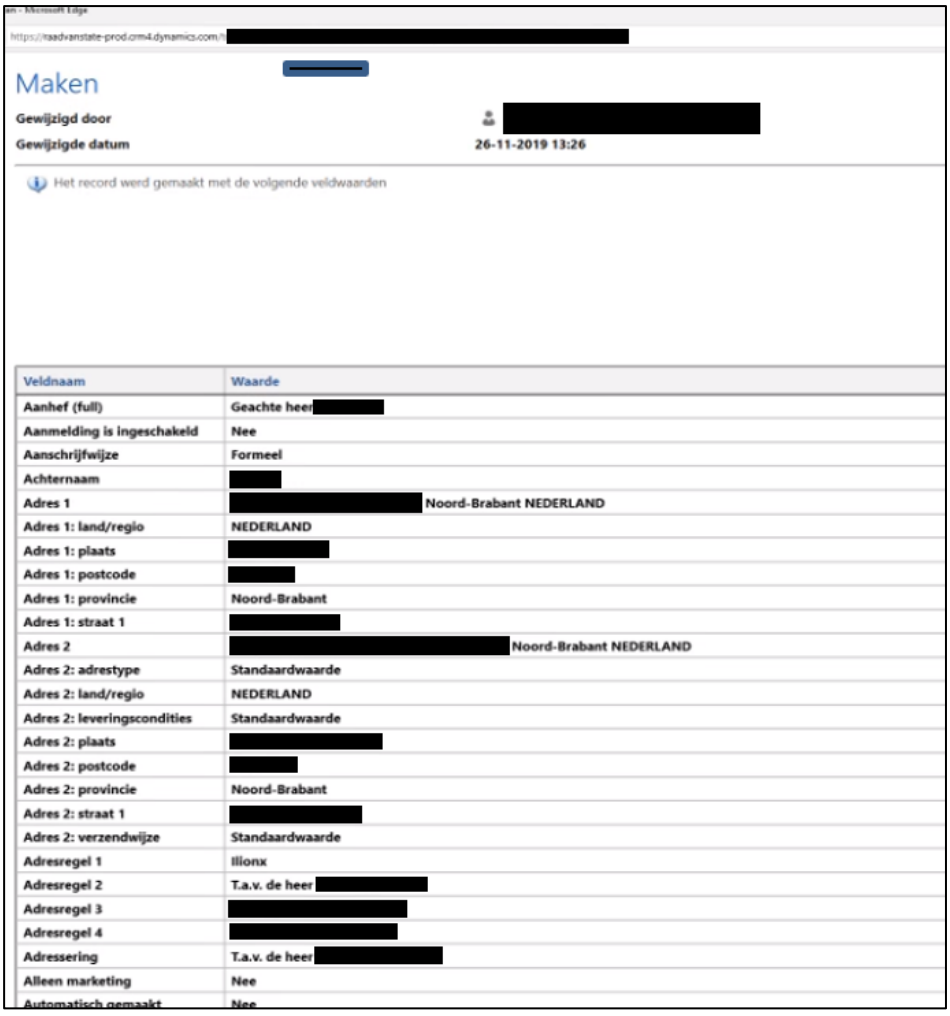


Figure 3 above shows an anonymized sample of a Create action in the Audit tables.

[18] Screenshot provided by the specific Dutch government organisation where the test set-up was made.

The Audit tables provide information which user accessed the system at what time and date, which user updated a field value of a record at what time and date, the previous field value before the update, which user deleted a record at what time and date, what locale was used to make an update, and a complete audit trail on a specific user's recent activities.[19]

System administrators have to actively enable the auditing feature. In the test setup this feature was turned on, with the retention period set to three months. The Audit tables can be deleted, paused, or restarted by a system administrator (or customized security role) to save storage capacity or for maintenance purposes.[20]

In reply to this DPIA, Microsoft explained that customers can limit the logging of Content Data, to prevent continued processing of sensitive or special categories of data in the audit logs.[21]

2.6.2 *Customer technical log files*

In the *on-premise* setup admins have access to technical log files with Diagnostic Data on their own server.

Microsoft explains these logs enable its customers to monitor "*server status and performance, troubleshooting issues, and planning for disaster recovery*".[22]

To examine the contents of the technical log files, a test scenario was run on the development environment of the *on-premise* Dynamics 365 system in 2019, and the relevant log files generated as a result of the execution of the test scenarios were analysed.

The Diagnostic Data in the log contained information on several levels of interaction with the application. While it was often not possible to tie the diagnostic information from the log files with certainty to actual events during the test session, the frequency of the logs often matched with the frequency of specific actions. For instance, it appears that for every new screen visited, a record was kept in one specific log file (2699055.json). This log file contained 93 records that could be related to the test session. It contained information referencing the user ID, the HTTP request and the web browser used. The sample did not contain any Content Data.

Across the different log files the following data types were recorded:

- Time of use (milliseconds)
- Location of data (EU, EMEA, 'westeurope')
- Browser information

---

[19] Microsoft, Audit data and user activity for security and compliance, 11 January 2021, URL: https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/audit-data-user-activity.

[20] Idem.

[21] Microsoft email 17 July 2023, with reference to the documentation, Enable or disable entities and fields for auditing, 16 February 2022, URL: https://learn.microsoft.com/en-us/dynamics365/customerengagement/*on-premise*s/admin/audit-data-user-activity?view=op-9-1#enable-or-disable-entities-and-fields-for-auditing.

[22] Microsoft, Operating Dynamics 365 Customer Engagement (*on-premise*s), 7 April 2023, URL: https://docs.microsoft.com/en-us/dynamics365/customerengagement/*on-premise*s/deploy/operating-microsoft-dynamics-365

- Agent
- Viewport
- Referrer
- IP address (possibly internal – encoded)
- User ID
- NPS status
- Current location ('none')
- Azure Active Directory status and ID
- Action

These data are personal data insofar as they relate to an employee. No personal data of other types of data subjects were detected in any of these log files.

The longest file (4461462.json) contained as many as 6.334 objects, much more than the number of distinct interactions made by the user during the test session. It appears to contain information about database access requests. It does not contain Content Data, but does include a UserRequestID, a SystemRequestID, a RequestID, and a CorrelationID, each with a unique identifier. These are not user identifiers. Nonetheless these identifiers might be linked by the government organisation to personal data in the database. This examination does not suggest that this data collection is excessive for the security purposes for which these logs are kept, as explained by Microsoft in the quote above.

Another file (3695963.json) contained 70 relevant records, that Privacy Company could not identify as connected to any specific user action. One of these 70 records contained a reference to a specific HTTP request that shows information is being transferred from the home.dynamics.com domain to the api.businessappdiscovery.microsoft.com domain, with the user ID and details about the used web browser. This sample record suggests user settings were somehow part of the interaction.

Most of the log files seem to register specific interactions. The contents of these logs are qualified as a logical and necessary measure to guarantee that any errors can be fixed and audit trails are created to detect intruders.

However, there was a reference in the log files to the Net Promotor Score, a metric for user satisfaction. The following snippet was recorded four times during the test session.

Figure 4: Net Promotor Score in logs


```
{
  "time": "",
  "correlationId": "",
  "properties": {
    "HasBeenPrompted": "False",
    "UserIdentifier": "XXXUSERPRINCIPALIDXXXX",
    "NPSSurveyType": "NPSInitial3DB"
  }
}
```

Microsoft did not explain why it had included this information in the logs. It could very well be a remnant of a functionality Microsoft doesn't use in the *on-premise* server, but only in the cloud service. It could also concern a functionality that has been switched off, or part of a functionality Microsoft makes available to its customers but was not activated in the test setup. Another option is that Microsoft only uses this functionality for other Enterprise customers, not for the Dutch government, to ask for Feedback from employee-users of the Dynamics services. Based on the framework agreement with the Dutch government, Microsoft is not allowed to process personal data for its own marketing purposes.

The technical inspection shows that Microsoft collects a variety of technical logs with limited information about the way employees interact with the *on-premise* Dynamics 365. These are personal data, but these data reveal little information about user activities.

The test scenarios included changing the contents of records about relations, but the logs did not include any references to the data subjects included in these Content Data.

The logs mostly contain limited descriptions of the actions of the users. Much of the data appear to be of little direct value from a practical point of view, such as security, without additional information on the contents of the action. For instance, one folder (named *2057*) in the logs contained 38 files, all created at the exact same time, containing the exact same information. The full contents are produced below in **Error! Reference source not found.** below.

Figure 5: full contents of log file


```
{
  "time":"2019-10-17T00:00:00-07:00",
  "correlationId":"VCoC2nCb/kmv6Gal",
  "properties":{
    "CustomerGroup":null,
    "ReferredByName":"",
    "ReferredByURL":null,
    "Market":"",
    "OSMarket":"",
    "OSLocale":"",
    "OSRegion":"",
    "ContentVertical":"",
    "RegionName":"",
    "CountryName":"",
    "Product":"No MSN Data Found",
    "OSName":"",
    "OSVersion":"",
    "Device":"",
    "Canvas":"",
    "Browser":"",
    "BrowserVersion":"",
    "ViewType":"",
    "ViewFeed":"",
    "ContentTitle":"",
    "DestinationUrl":"",
    "UserAction":""
  }
}
```

The only meaningful data in this example are the correlationID and the Product. To record this information 38 times does not seem relevant for any business purpose.

The log files suggest that some data are being stored within the EU, when the field 'Geo' contains 'EUR', while other data might be stored in the EMEA (Europe, Middle East, Africa), when the same field contains 'EMEA'. However, in an *on-premise* setup, no log files are being sent to Microsoft. It is thus unclear why the log files contain a geo indication.

Additionally, Microsoft offers a range of optional monitoring features to its customers. Customers can switch these services on, or install add-ons to *on-premise* Dynamics 365. These features are out of scope of this DPIA.

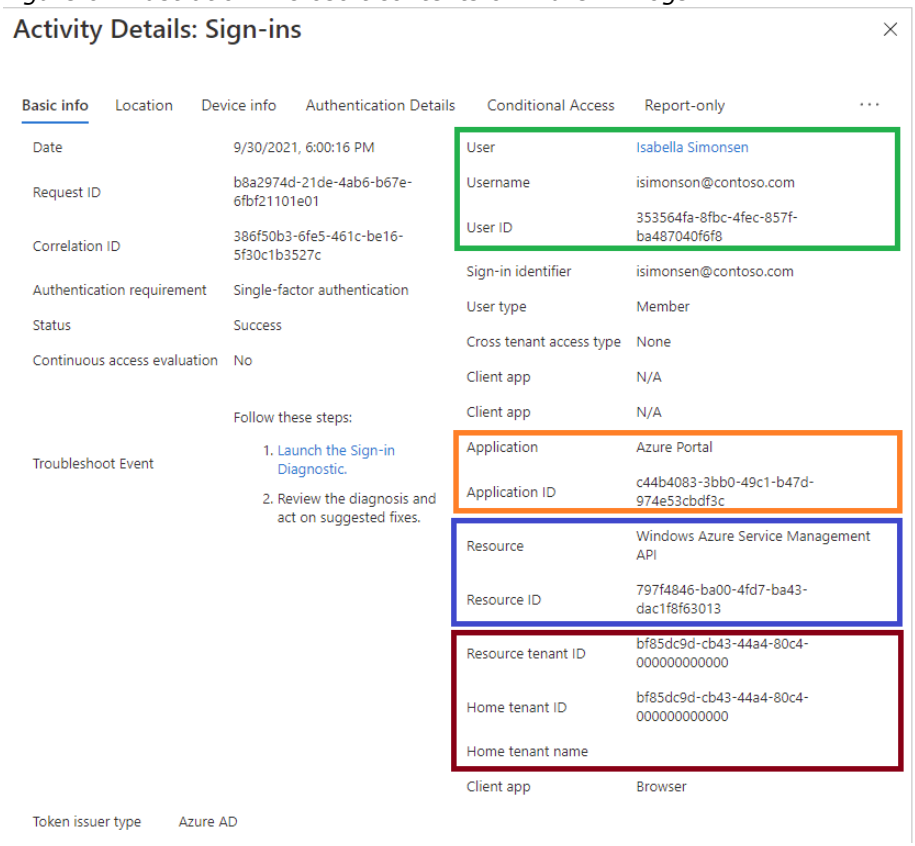
2.6.3 Azure AD audit logs

Though Privacy Company did not obtain access to the Azure AD audit logs Microsoft provides to its customers, a short description is provided here, based on Microsoft's public documentation.

The logs offer an overview of sign-in activity from all employees. Admins can review sign-in errors and patterns.

Microsoft shows a list of all basic information collected with each call to the Azure AD.

Figure 6: Illustration Microsoft contents of Azure AD logs



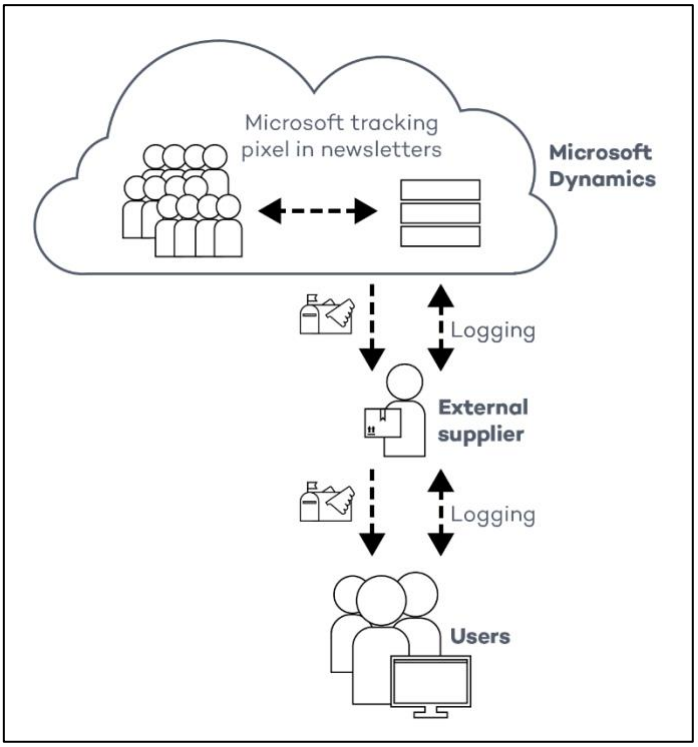
Microsoft explains that admins can check the interactive user sign-in logs for the following activities:

- "A user provides username and password in the Azure AD sign-in screen.
- A user passes an SMS MFA challenge.
- A user provides a biometric gesture to unlock their Windows PC with Windows Hello for Business.
- A user is federated to Azure AD with an AD FS SAML assertion.
-
- In addition to the default fields, the interactive sign-in log also shows:
-
- The sign-in location
- Whether Conditional Access has been applied."[23]

2.6.4 *Customer logs about tracking pixel in newsletters*

When newsletters and other mailings are sent directly from *on-premise* Dynamics 365 to a list of recipients, by default *on-premise* Dynamics 365 will include a tracking pixel in the body of the emails sent out. This tracking pixel informs *on-premise* Dynamics 365 whether and when the recipient has opened the email. The tracking pixel is meant to be activated when the user reads the email. The pixel contains a specific identifying code, which makes it possible to see for Microsoft and its customers which recipients have opened the mail unless the customer turns this pixel off.

Figure 7: Tracking pixel process flow



Since not all recipients use a mail client that will open the pixel by default, the resulting reading behaviour statistics are not accurate. The customer cannot conclude for sure a recipient has not opened the email.

[23] Microsoft, Sign-in log in Azure Active Directory (preview) 28 March 2023, URL: https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-all-sign-ins?source=recommendations#interactive-user-sign-ins

The server logs of the *on-premise* Dynamics 365 register every attempt to open the newsletters if the pixel is activated according to the scheme shown above in Figure 7.

In reply to the initial findings of the DPIA, in 2020 Microsoft created a new option for customers of the Marketing Module to disable the tracking pixel.[24] The new option is available in the versions of Dynamics released after June 2020.[25] The new option was not yet available in the test setup version, but Privacy Company did test the new option for another customer, and confirmed that the setting was effective and did prevent inclusion of the tracking pixel.

An organisation can choose to disable the pixel completely, or allow recipients to opt-out. In that case the pixel is still set and read, but translated in an anonymous click.

Microsoft explains:

> *"When the recipient selects a link or opens a message with a tracking pixel, two things happen:*
>
> *The recipient is redirected to the original URL.*
>
> *The link click interaction is recorded.*
>
> *If the recipient previously opted out from tracking, the interaction is generated as anonymous. When the recipient has opted out, the interaction doesn't store a customer profile reference.*"[26]

2.6.5 *Microsoft logs about the use of the Azure AD*

In the test setup Microsoft did not provide access to the logs it keeps about the use of its Azure AD. It is not clear if this lack of reply was due to the fact that Microsoft had already anonymised these data in its own logs, or if the DSAR request was lost, in spite of a reminder.

In reply to this DPIA, Microsoft provided a URL with information about its current approach to such requests in the context of Dynamics 365.[27] The page describes the possibilities for admins to export or delete Content Data, and the possibilities to export system generated server logs. According to the description, this includes access to Azure AD audit logs, that is, the logs that Microsoft makes available to admins.

Privacy Company did not file a renewed data subject access request, because it does not expect discrepancies with the documented contents of these audit logs.[28] However, this access does not include the personal data Microsoft processes for its own security purposes.

---

[24] Microsoft, Enable GDPR features in Dynamics 365 Marketing, 7 July 2023, URL: https://docs.microsoft.com/en-us/dynamics365/marketing/gdpr#view-and-set-the-consent-level-for-each-contact.

[25] As confirmed by Microsoft to Privacy Company in an e-mail from 5 June 2020.

[26] Microsoft, Real-time marketing link tracking mechanics, 1 August 2023, URL: https://learn.microsoft.com/en-us/dynamics365/marketing/real-time-marketing-link-tracking-mechanics.

[27] Microsoft, Dynamics 365 Data Subject Requests for the GDPR and CCPA, 4 April 2023, URL: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-dynamics365 .

[28] Microsoft, Azure AD audit log categories and activities, 16 March 2023, URL: https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-audit-activities

As described in an earlier DPIA on Microsoft's Office for the Web and mobile Apps[29], Microsoft collects and processes two types of personal data about the use of the Azure AD. The first category consists of log files that Microsoft collects and processes for its own purposes for auditing, research, user analysis, software debugging, system health analysis and system-wide analysis using machine learning. Microsoft indicates that these files contain usernames. Microsoft writes that it removes personal data from the log files (scrubbing) before processing the data in the machine learning systems for general analysis.

Microsoft writes: "*Log files contain data about usernames, groups, devices, and apps. Log files are originally created and stored in Azure storage in the data center where the Azure AD service runs. Log files are used for local debugging, usage analysis, and system health monitoring purposes, as well as for service-wide analysis. Prior to any system-wide analysis, log files are first scrubbed of personal data, which is tokenized. These logs are then copied over a secure SSL connection to Microsoft's reporting machine learning systems, which are contained in Microsoft owned data centres in the Continental United States.*"[30]

In addition, Microsoft describes that it collects a category of 'Usage data' on the Azure AD. Not only for the customers, but also for themselves, in order to analyse system usage and to be able to improve the service. Microsoft says that it will first delete the personal data in this category.

Microsoft writes: "*Usage data is metadata generated by the Azure AD service that indicates how the service is being used. This metadata is used to generate administrator and user facing reports and is also used by the Azure AD engineering team to evaluate system usage and identify opportunities to improve the service. This data is generally written to log files, but in some cases, is collected directly by our service monitoring and reporting systems. personal data is stripped out of Microsoft's usage data prior to the data leaving the originating environment.*"[31]

Use of the Azure AD means some personal data are accessible from the USA. This transfer is described in Section 7 of this report.

2.6.6 Microsoft Telemetry Data from the on-premise server

In reply to this DPIA, Microsoft explained that older, pre-GDPR configurations of the *on-premise* servers can send some Telemetry Data to Microsoft. Microsoft explained that these are Software Quality Metrics data ("SQM") that Microsoft no longer uses.[32]

---

[29] SLM Rijk, DPIA Office 365 for the Web and mobile Office apps (March 2020), version 1.1, URL: https://slmmicrosoftrijk.nl/wp-content/uploads/2021/07/200630-DPIA-Office-for-the-Web-and-mobile-Office-apps.pdf.

[30] Microsoft, Azure Active Directory Data Security Considerations - Download Center, version 2.02, June 2020, URL: http://download.microsoft.com/download/A/A/4/AA48DC38-DBC8-4C5E-AF07-D1433B55363D/Azure-AD-Data-Security-Considerations.pdf. Microsoft refers to its up to date page on Data residency for the Azure AD, 6 February 2023, URL: https://learn.microsoft.com/en-gb/azure/active-directory/fundamentals/data-residency.

[31] Ibid.

[32] The only publicly available information Privacy Company could find dates from 2013, and contains an extensive description of SQM data collected from Dynamics *on-premise* 2013. 5 Microsoft Dynamics CRM Client counters, URL: https://download.microsoft.com/download/D/4/4/D4427B9E-7D1F-4F73-9C75-8F03673697C8/Performance%20Counters%20for%20Microsoft%20Dynamics%20CRM%202013.pdf.

Microsoft recommends admins to centrally deactivate this data collection by blocking access to the receiving Microsoft domains. The *on-premise* Dynamics server does not have any required Telemetry Data, as this software is designed to offer air gapped deployment if that is what the customer wants. Therefore, network admins can block MS endpoints on their network so that no data are sent to Microsoft.

Microsoft explains that doing this will not impact the functionality of the *on-premise* Dynamics 365 product solution itself, but there may be other disadvantages if the same users or servers are dependent on cloud services at Microsoft. Deactivation could also mean the solution owner needs to deal with software updates itself, if blocking means access to automated updated capability is blocked.

Microsoft warns:

> "*Organizations are advised to proceed with caution, making small interventions and testing for impacts in an incremental approach. If there is an impact on one or more aspects of other cloud functionality or on software, then this shows what elements were giving rise to the data communication with Microsoft.*"[33]

As a result of the dialogue with SLM Rijk, Microsoft has provided specific policy rules for admins to block the sending of the Telemetry Data. These rules are included in Annex 1.

2.6.7 Authentication cookies collected by Microsoft

As described in Section 2.5, the *on-premise* deployment was combined with use of Microsoft's cloud service Azure AD for authentication purposes. This meant employees had to visit the online Microsoft log-in page to authenticate themselves for access to the *on-premise* server via their browser. In the test setup there was no other access option (no installed apps on devices). Because the browser needs to send its authentication information in each request (without cookies, the http connection is *stateless*), Microsoft has to use functional cookies to remember the user.

The intercepted data traffic only showed traffic to Microsoft-owned domains and specifically, access to the Dynamics server, but no traffic to third parties. The traffic does contain cookies with unique identifiers, but these cookies can be qualified as functional cookies to transmit the authentication request. Therefore, as will be explained in more detail in Section 9 of this report, prior consent is not required.

It follows from the intercepted outgoing traffic that Microsoft -at least- collects the following personal data through these functional cookies:

- IP-address
- Time of access
- User Agent
- Referrer
- ID in header x-ms-RefreshTokenCredential
- ClientID
- Value with unique number

[33] Email Microsoft to SLM Microsoft, AWS and Google Rijk, 17 July 2023.

- Login_hint in the format of an e-mail address[34]

An example of such a functional cookie with a retention period of 1 day is shown in Figure 8 below.

Figure 8: Contents of functional cookie


```
{
  "name": "fpc",
  "value": "[unique number removed]",
  "path": "/",
  "domain": "login.microsoftonline.com",
  "expires": "2020-10-18T10:14:57.000Z",
  "httpOnly": true,
  "secure": true,
  "sameSite": "None"
}
```


Other examples of cookies with non-unique identifiers are shown in Figure 9 below.

Figure 9: Example of cookie with non-unique identifiers


```
{
  "name": "x-ms-gateway-slice",
  "value": "estsfd",
  "path": "/",
  "domain": "login.microsoftonline.com",
  "expires": null,
  "httpOnly": true,
  "secure": true,
  "sameSite": "none"
},
{
  "name":   "stsservicecookie",   [security   token   service   cookie,
explanation added by Privacy Company]
  "value": "estsfd",
  "path": "/",
  "domain": "login.microsoftonline.com",
  "expires": null,
  "httpOnly": true,
  "secure": true,
  "sameSite": "none"
}
```


Microsoft appears not to publish any documentation about the contents and purposes of cookies used on the log-in page for Dynamics. Microsoft only makes information available about cookies that can be used by customers in the Dynamics marketing module.[35] Customers can disable non-essential cookies, see Section 3.3 below.

Separate from these cookies, Microsoft also logs access to its Azure AD in Azure security logs, as described in Section 2.3 above.

---

[34] This is not a limitative list of all data collected by Microsoft through these cookies, but this list shows the clearest examples of personal data.

[35] Microsoft, How Dynamics 365 Marketing uses cookies, 8 January 2023, URL: https://docs.microsoft.com/en-gb/dynamics365/marketing/cookies

2.6.8 *Unrelated application Telemetry Data*

In additional testing, Privacy Company observed that some Telemetry Data were sent from the browser to Microsoft when using *on-premise* Dynamics 365. These Telemetry Data did not contain directly identifiable personal data but did sometimes include unique user IDs. The browser created POST requests, sending telemetry events with data in the body of the request to the server https://browser.pipe.aria.microsoft.com/. Privacy Company captured traffic to that server and additional tests were conducted to generate more Telemetry Data. The following requests were captured over a total of 32 POST requests (most POST requests contained more than one telemetry event):

Table 1: Telemetry data requests to Microsoft when using a browser

Event name	**Frequency**
uci_monitor_performance	20
uci_monitor_success	32
uci_trace	94
initializelivepersonacard_success	2
uci_context	18
livepersonacard_configurationsetaction	2
uci_monitor_failure	10
awt_stats	10

At least in the two cases of calls to "livepersonacard_configurationsetaction", the call contained the unique user ID and other identifying data.

In reply to this DPIA, Microsoft explained that these Telemetry Data were not collected from the *on-premise* Dynamics 365 software. These observed Telemetry Data were the result of integration with other Microsoft cloud services in the test setup, such as the Azure AD, SharePoint Online and Exchange Online for e-mail.

Microsoft explained:

> "*In the DPIA document and in the table above there are references to "livepersonacard" attributes and to the URI https://browser.pipe.aria.microsoft.com/. These are not aspects of D365 CRM, but of* ***other*** *Microsoft software and cloud functionality.*
>
> *"Livepersonacard" is functionality of Microsoft cloud productivity services (Exchange Online Email, SharePoint Online content management, Power Platform PowerApps). The "Aria" URI is an exposed endpoint for the collection of Diagnostic Data, that is used by Microsoft software that does so.*
>
> *Microsoft's conclusion from the appearance of these aspects in the DPIA testing work is that the platform tested was integrated with cloud-based productivity services. While this is a valid configuration, evaluating it alongside D365 CRM adds confusion to consideration of the privacy baseline of D365 CRM software; considerations are introduced that were based on deployment choices by the deploying organization, and that exceed the considerations for D365 CRM alone.*"[36]

[36] Email Microsoft to SLM Microsoft, Google and AWS Rijk, 17 July 2023.

3. Privacy controls

Microsoft offers several privacy controls for admins when a government organisation uses the *on-premise* Dynamics software in combinatie with the (optional) Azure AD.

3.1 Exclude sensitive data from the Audit tables

Government organisation are advised not to record sensitive data attributes or special categories of data in the Audit tables.

Microsoft documents the different configuration options for organisations to configure the logs and Audit tables in a GDPR-compliant way when setting up Dynamics 365. [37] These options must be configured when the solution implementation is designed. Microsoft also offers functionality to delete records from the audit log relating to relations that have been deleted from the Content Data.[38]

3.2 Remove outdated data from the Azure AD (Content and Diagnostic Data)

Microsoft also offers functionality to delete (former) employees as CRM users and remove all references to them in the audit log. Microsoft recommends to replace personal data in the user entity records with 'null' or 'non-personal data' in stead of removal, to maintain audit record fidelity. By using this replacement approach, the audit log will still show the "CRUD" activities performedon the database records but will simply show the newly nullified data for the user that performed the "CRUD".

Microsoft has ensured such a replacement is effective: "In the auditing software design, the references to the D365 CRM user that the audit log shows are obtained from cross-reference to the user directory and are not copied into the audit logs."[39]

Note: as the set-up is often done by an external partner, government organisations are advised to include the correct GDPR compliant configuration of the logs and Audit tables in the contract with the partner, as retro-fitting may be costly.

3.3 Display internal privacy policy to employees and guest users

Organisations can process a lot of personal data through Dynamics 365. By using an internal privacy policy, the organisation is able to explain what employees are and are not allowed to do with the personal data in the CRM, en what rules the organisation applies to access to the Diagnostic Data about the use of the software.

Microsoft provides the option to show the internal privacy policy on the login page, and to enforce accepting the internal privacy policy via Azure AD, including, e.g., for guest users in Teams.

- Start at https://admin.microsoft.com -> Settings -> Org Settings -> Security & privacy -> Privacy Profile.

---

[37] Microsoft, Enable or disable entities and fields for auditing, 16 February 2022, URL: https://learn.microsoft.com/en-us/dynamics365/customerengagement/on-premises/admin/audit-data-user-activity?view=op-9-1#enable-or-disable-entities-and-fields-for-auditing

[38] Microsoft, Recover database space by deleting audit logs, 15 June 2022, URL: https://learn.microsoft.com/en-us/power-platform/admin/recover-database-space-deleting-audit-logs.

[39] Microsoft reply to the DPIA, 17 July 2023.

- Add a link to the login page for employees tot he internal privacy policy, to provide employees with information about the policy, including the rules for the use of log files. (see Figure 10 up to, and including Figure 13 below).
- Enforce accepting via Azure AD (see Figure 14 en Figure 15 below).

Figure 10: Settings enforcing displaying internal privacy policy (1)

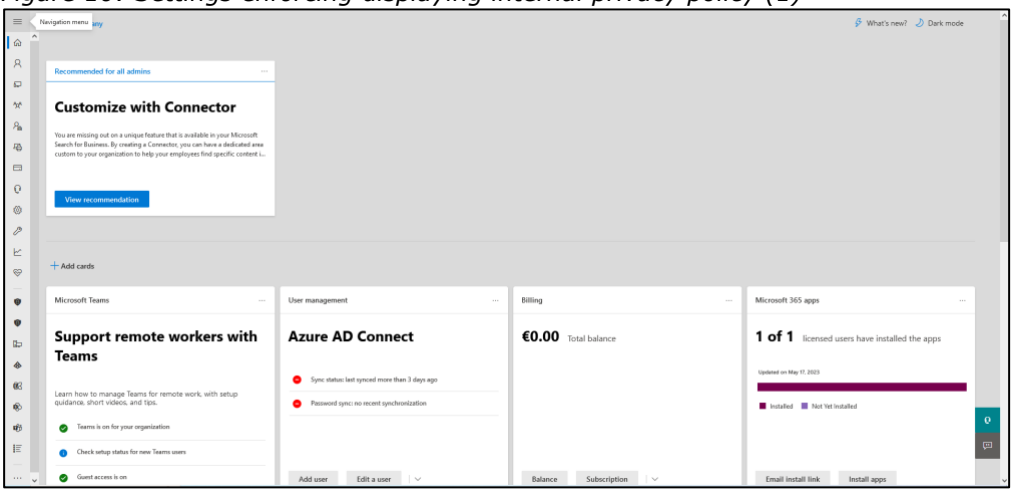


Figure 11: Settings enforcing displaying internal privacy policy (2)

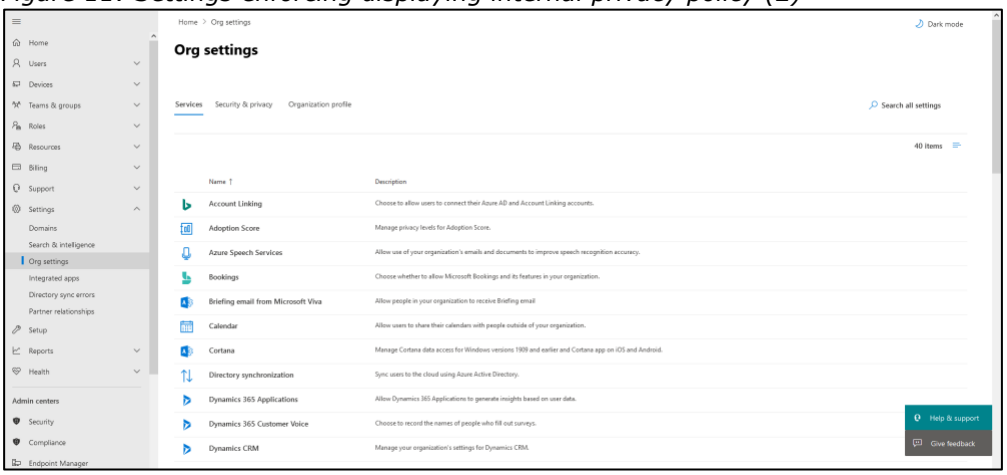


Figure 12: Settings enforcing displaying internal privacy policy (3)

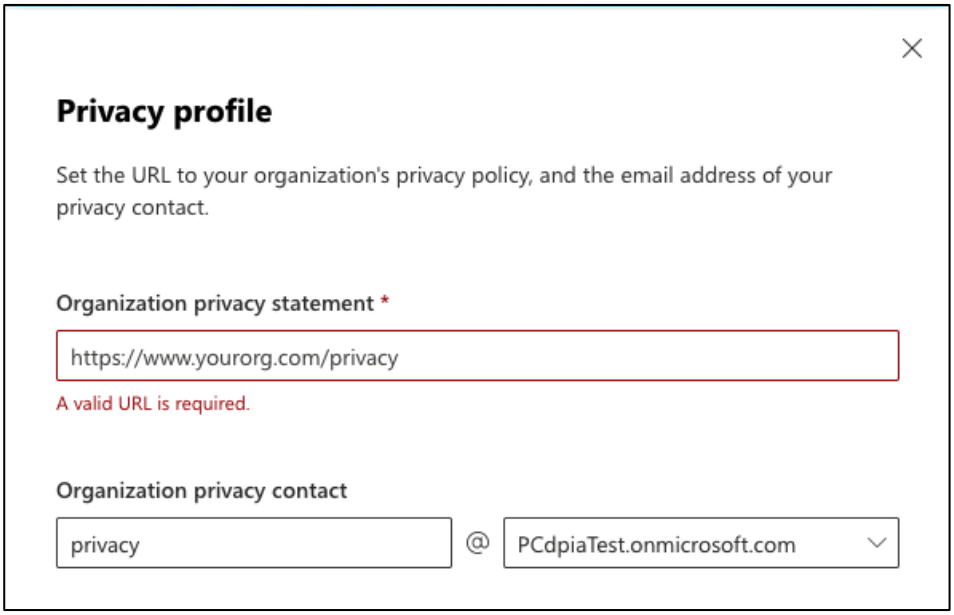
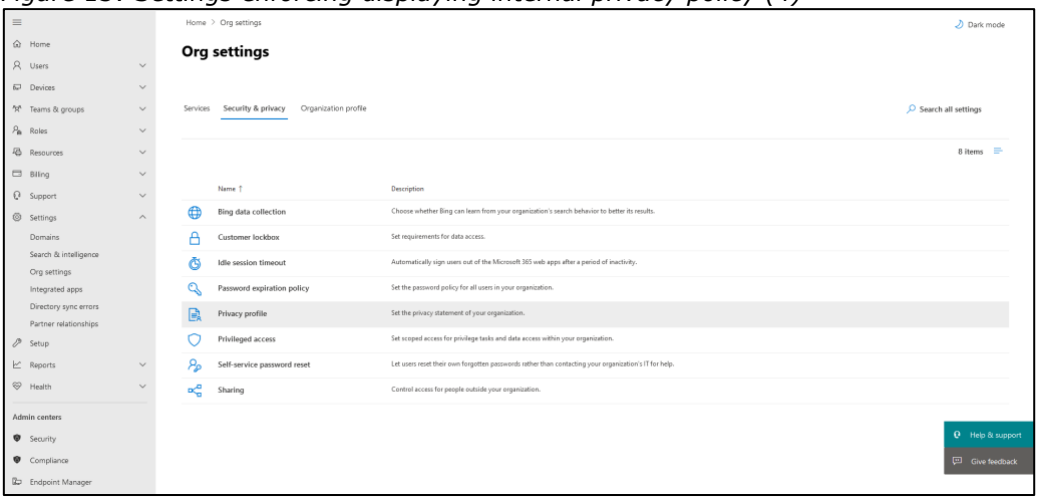


Figure 13: Settings enforcing displaying internal privacy policy (4)



As part of the Conditional Access options, the Azure AD can be instructed to force end users to accept the internal privacy policy of the (government) organisation. Such a Conditional Access policy can be enforced after first-factor authentication has been completed. This way, administrators can increase awareness of relevant privacy rules with end users.

- Go to https://portal.azure.com/ -> type "Conditional access" in the search bar -> "Terms of use" on the left -> new terms.
- Enable the Conditional Access options for the Azure AD.

Figure 14: Conditional Access options Azure AD (1)

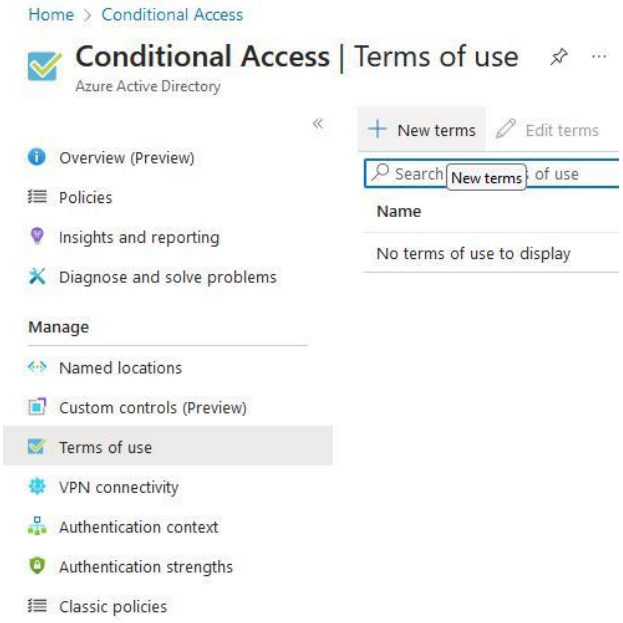
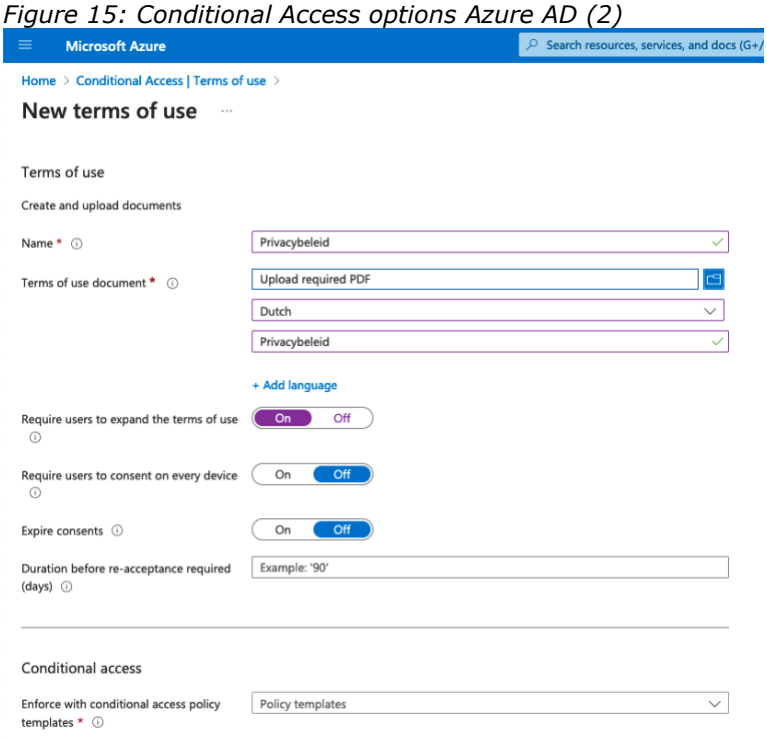


Figure 15: Conditional Access options Azure AD (2)



3.4 Pseudonymise account information of admins / employees

If government organisations work with secret or highly confidential data, they may want to keep the identity of their admins confidential. There are two options:

1. Do not use the Azure AD, but use the local AD for authentication, or:
2. Use a pseudonym in the Azure AD for specific employees if necessary, for example, admin01@[governmentdomainname.nl].

Pseudonymisation can be done in the Azure AD, even if it is being used as Single Sign On to services of other companies. The organisation can also choose to create generic accounts for system administrators (systemadmin1@orgx, etc.)

3.5 Block server Telemetry Data (in pre-GDPR Dynamics 365 versions)

Admins are advised to centrally deactivate Microsoft's server Telemetry Data collection by applying the policy rules included in Annex 1.

As explained above, in Section 2.6.5, the *on-premise* Dynamics server does not have any required Telemetry Data. Network admins can also attempt to block MS endpoints on their network so that no data are sent to Microsoft, but this may conflict with user interface and architecture requirements. As a consequence of such blocking, admins must perform manual security and performance updates of the *on-premise* software.

3.6 Ask for consent or disable the tracking pixel in newsletters

Microsoft enables organisations to ask for consent for the use of a tracking pixel per contact.[40] If a user does not provide consent, the interaction is generated as anonymous. Organisations can also centrally disable the tracking pixel in the Marketing Module for all contacts, by changing the compliance profile for all relations to 'Not tracked'.[41]

3.7 Disable non-essential Marketing cookies

If a government organisation uses the Dynamics 365 Marketing Module on its website, by default Microsoft sets non-functional cookies. Organisations that do not wish to ask for consent from their website visitors can disable the non-essential cookies by adding a short script to their website.

Figure 16: Script to block non-essential Marketing cookies

```
<script>
  function d365mktConfigureTracking() {
    return {Anonymize: true};
  }
</script>
```

Microsoft warns that users will appear to be anonymous. Organisations can still use forms to invite users to provide identifying data, but the function of form pre-fill data will not work.[42]

3.8 Minimise the Telemetry Data from Windows 10/11

As described in Section 2.5.5 above, Microsoft can log usage of the *on-premise* Dynamics 365 if such an activity is captured by the Telemetry Data sent to Microsoft from the operating system, such as Windows 10 or 11 or Office 365.

This DPIA assumes all government organisations follow the recommendation from SLM Rijk to set the telemetry level in Windows and Office 365 to the least invasive

---

[40] Microsoft, Outbound marketing compliance settings, 7 July 2023, URL: https://learn.microsoft.com/en-us/dynamics365/marketing/privacy-use-features.

[41] Microsoft, Consent to track user behavior, URL: https://learn.microsoft.com/en-us/dynamics365/marketing/real-time-marketing-email-text-consent.

[42] Microsoft, How to disable non-essential Dynamics 365 Marketing cookies, 3 June 2023, URL: https://learn.microsoft.com/en-gb/dynamics365/marketing/cookies#how-to-disable-non-essential-dynamics-365-marketing-cookies.

'security' level. In that case, such activity data will not be captured, and are therefore out of scope of this DPIA.

The default setting for Windows telemetry is that both Required and Optional Diagnostic Data are enabled, but users are given the choice to disable Optional Diagnostic Data.

Administrators can centrally minimise the data processing via Windows Telemetry Data. Microsoft offers three choices, similar to the choices for Office 365:

1. Disabled
2. Required
3. Optional

With a higher telemetry level in Windows, Microsoft can also collect more data on the individual use of the Dynamic application.

If organisations use centrally managed devices with images of the required software, they can set the telemetry level in the end-user drop-down menu as follows:

- In Windows 10, -> Settings > Privacy > Diagnostics & feedback.
- In Windows 11 -> Settings > Privacy & security > Diagnostics & feedback.

It is also possible to set the telemetry level via the Registry Editor or a group policy:

- From the Group Policy Management Console, go to Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds.
- Double-click Allow Telemetry (or Allow diagnostic data on Windows 11 and Windows Server 2022) and select 'disabled'.[43]

[43] Microsoft, Use Group Policy to manage diagnostic data collection, 18 March 2023, URL: https://learn.microsoft.com/en-gb/windows/privacy/configure-windows-diagnostic-data-in-your-organization#use-group-policy-to-manage-diagnostic-data-collection

Figure 17: Options telemetry Windows 10 and Windows 11 (Renamed policy)[44]

Policy type	Current policy	Renamed policy
Group Policy	Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds >**Allow Telemetry** • **0 - Security** • **1 - Basic** • **2 - Enhanced** • **3 - Full**	Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds >**Allow Diagnostic Data** • **Diagnostic data off (not recommended)** • **Send required diagnostic data** • **Send optional diagnostic data**
Group Policy	Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds >**Configure telemetry opt-in settings user interface**	Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds >**Configure diagnostic data opt-in settings user interface**
Group Policy	Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds >**Configure telemetry opt-in change notifications**	Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds >**Configure diagnostic data opt-in change notifications**

3.9 Minimise the Telemetry Data from Office 365

Similar to the Windows telemetry minimisation options, Microsoft offers three options for setting telemetry levels in Office 365:

1. Required
2. Optional
3. Neither[45]

Even at the minimum level, 'Neither,' Microsoft still collects Telemetry Data. Microsoft refers to these data as 'Required Service Data for Office'.[46] This dataflow contains information about the use of 'connected experiences' the organisation uses, as well as information about essential Office services, such as the licensing service which tells Microsoft if a user has the right license to use Office.

SLM Rijk recommends minimising the data traffic via telemetry from Office services by setting telemetry to the 'Neither' level. By choosing this option (instead of 'Required'), Microsoft processes fewer sensitive data. It is possible to minimise the data flow with a Group Policy via User Configuration\Policies\Administrative Templates\Microsoft Office 2016\Privacy\Trust Center.[47]

- Go to https://config.office.com, Select 'Office policies' **->** Go to Microsoft 365 Cloud Policy -> Search for the policy *Configure the level of client software diagnostic data sent by Office to Microsoft* -> Enabled.

[44] Microsoft, Changes to Windows diagnostic data collection, 18 March 2023, URL: https://learn.microsoft.com/en-gb/windows/privacy/changes-to-windows-diagnostic-data-collection

[45] Microsoft, Diagnostic data sent from Microsoft 365 Apps for enterprise to Microsoft, 28 March 2023, URL: https://learn.microsoft.com/en-gb/deployoffice/privacy/overview-privacy-controls#diagnostic-data-sent-from-microsoft-365-apps-for-enterprise-to-microsoft.

[46] Microsoft, Required service data for Office, 4 April 2023, URL: https://learn.microsoft.com/en-gb/deployoffice/privacy/required-service-data.

[47] Microsoft, Use policy settings to manage privacy controls for Microsoft 365 Apps for enterprise, 27 March 2023, URL: https://learn.microsoft.com/en-us/deployoffice/privacy/manage-privacy-controls.

Figure 18: Disabling collecting Office Telemetry Data (1)

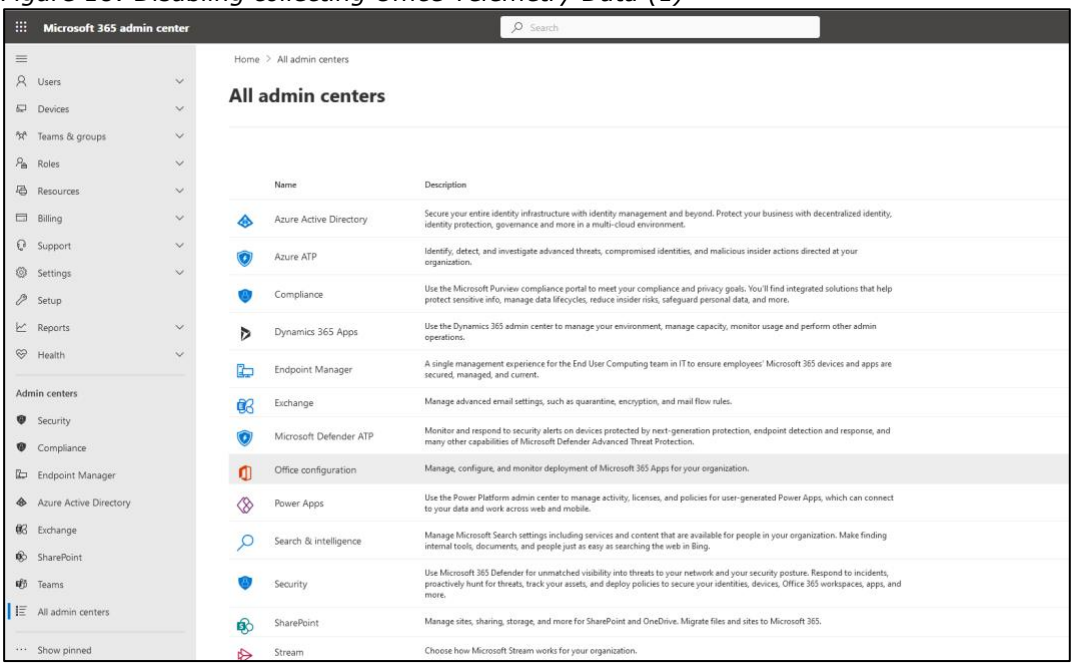


Figure 19: Disabling collecting Office Telemetry Data (2)

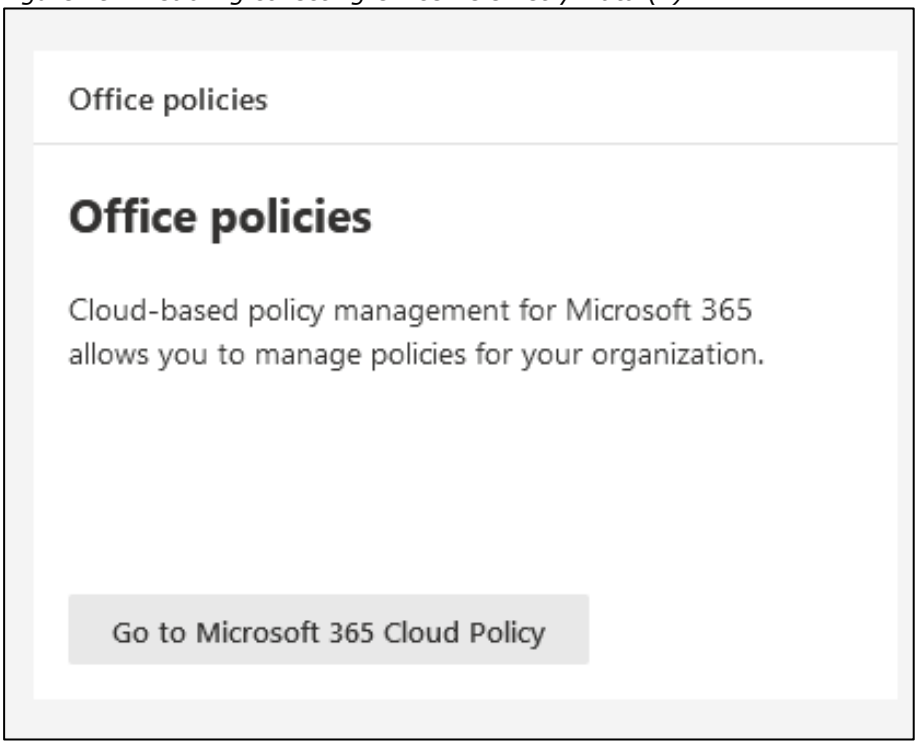
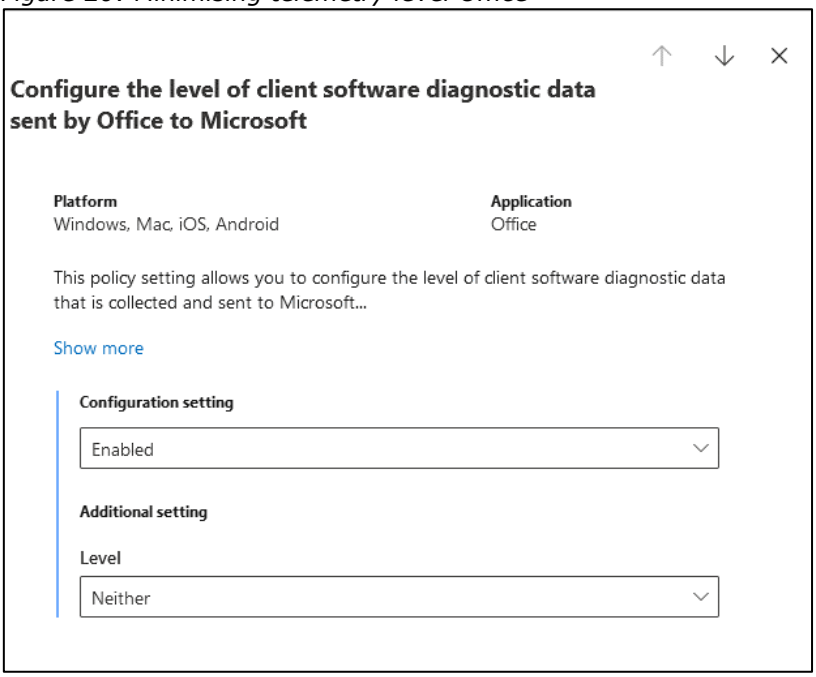


Figure 20: Minimising telemetry level Office



4. Purposes of the Processing

This section describes the different purposes of the processing by government organisations, and by Microsoft.

4.1 Purposes determined by the government organisations

In the test setup, personal data in the *on-premise* Dynamics 365 and the Azure AD were processed for 11 specific purposes. The first six purposes are related to the processing of personal data from external data subjects, the last five purposes are related to the authentication of employees and security requirements.

1. Relationship management, entry, updating and manual deletion of contact information about relations of the government organisation.
2. Verification of the address data in the CRM system, through the use of an external online service.
3. Creating back-ups of the database.
4. Organisation of meetings and events, segmentation of contacts and sending of letters and (e-)mail(ing)s.
5. Remembering food preferences: Taking into account self-provided dietary preferences of relations visiting customer organised events.
6. Tracking of newsletter reading with pixels.
7. Administration of the system, including setting up roles for specific users and their permissions.
8. Authentication and authorisation of employees with the Azure AD.
9. Logging of changes made to specific records (with the Audit tables).
10. General security purposes (detection of unlawful access and data breaches with the technical logs and the Audit tables, including the creation of back-ups of the database).

11. Removal of obsolete personal data from the Audit tables (individually or by date range).

4.2 Purposes determined by Microsoft

The improved privacy terms in the framework contract between the Dutch government and Microsoft for the Online Services (including browser accessed and mobile applications) **do not apply to the Dynamics 365 *on-premise* software**, as the framework contract applies to Online Services.

Based on the Product Terms for Dynamics 365 *on-premise* Microsoft does not offer any Service Specific Terms for Dynamics 365 *on premise*.[48] Only Microsoft's universal license terms apply, and these do not include purposes of the processing.[49] The universal license terms state that the Data Protection Addendum may apply if Microsoft is a processor of subprocessor of personal data in connection with a software product. Absent such a data processor commitment in Specific Service Terms, Microsoft's 18 data controller purposes from its general Privacy Statement apply.[50] In discussions with SLM Rijk, Microsoft confirmed that the role of Microsoft was unclear.[51]

Microsoft has explained that the only data it collects from the pre-2018 installs of the *on-premise* server are Telemetry Data for Software Quality Management (SQM), even though the data are no longer used for any purpose.

"SQM data is no longer being processed at Microsoft and any such agent discovered should be disabled by customers. Please note that an administrator or a user previously enrolling in Microsoft's various Customer Experience Improvement Programs (CEIP) may also activated SQM collection agents or required them installed."[52]

If admins apply the recommended policy included in Annex 1 to block the obsolete Telemetry Data from pre-2018 *on-premise* servers, no data are shared with Microsoft, and hence, Microsoft does not have any processing purposes.

The improved framework contract with the Dutch government **does apply to the processing of personal data resulting from use of the Azure AD**, both the Azure AD logs, and the cookie data for authentication purposes.

The Dutch government privacy amendment stipulates that Microsoft may only process the personal data that it obtains from, about, or via the use of its Online Services for three authorised purposes, and only when proportional. These purposes are:

1. to provide and improve the service,
2. to keep the service up-to-date and
3. secure.

---

[48] Microsoft licensing terms for Dynamics 365 On-premises, URL: https://www.microsoft.com/licensing/terms/productoffering/MicrosoftDynamics365Onpremises/all.

[49] Microsoft universal licensing terms, URL: https://www.microsoft.com/licensing/terms/product/ForallSoftware/all

[50] Microsoft Privacy Statement, last updated July 2023, https://privacy.microsoft.com/en-us/privacystatement.

[51] Conference call Microsoft, SLM Rijk and Privacy Company, 16 August 2023.

[52] Microsoft reply to the DPIA, 17 July 2023.

The Dutch government and Microsoft have also agreed that Microsoft may never process personal data from Dutch government customers for the following purposes:

1. Data analytics
2. Profiling
3. Advertising or similar commercial purposes, including targeted on-screen recommendations for Microsoft products or services that the customer does not use
4. Market research aimed at developing new functionalities, services or products.

Additionally, SLM Rijk and Microsoft have agreed that Microsoft is permitted to further process some personal data as data controller, when necessary, for a limitative list of Microsoft's own legitimate business purposes. These purposes range from the obvious (sending invoices, creating statistics for the annual financial reports) to the often forgotten, such as mandatory disclosure to law enforcement when Microsoft is not allowed to redirect a request to its customer.
forgotten, such as complying with orders from law enforcement.
In March 2021, SLM Rijk published the results of the first audit on Microsoft's compliance with these processing limitations, in particular the prohibition on profiling.[53] This did not result in any findings about non-conformities.

5. Controller, Processor, and Subprocessors

The different legal roles of the involved (commercial) parties in the processing of personal data are defined in Article 4 (7) to (4) 9 GDPR.

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

5.1 The role of the government customer as data controller

Government customers can determine and decide what Content Data they process in the *on-premise* Dynamics 365 software. Customers can also decide on the scope of their internal processing of Diagnostic Data on the use of the software, for example by excluding sensitive data from the Audit tables, or by deleting former employees from the logs. Because they are able to take these decisions on the scope of the processing, the government organisations factually and formally qualify as data controllers.

As controllers, government organisations can also block the sending of Telemetry Data to Microsoft, with the policy provided in Annex 1. If admins do not use this policy, Microsoft becomes data controller for these data. See Section 5.3 below.

---

[53] See the website of SLM Rijk, for the full audit reports in Dutch and English. Memo from SLM Rijk, https://slmmicrosoftrijk.nl/wp-content/uploads/2021/04/20210408-Memo-Audit-EY-Microsoft-2020-ENG-pdf.pdf. Summary EY of audit report in English: https://slmmicrosoftrijk.nl/wp-content/uploads/2021/04/REQ5267448-B-MinJen-V-Summary-report-Profiling-restrictions-Microsoft-final-wq-versie.pdf

Government organisations can block the inclusion of a tracking pixel in newsletters they send with the (online) Dynamics marketing module. Even though Microsoft shows a warning that organisations are responsible to obtain consent from customers for cookies (and tracking pixels), legally Microsoft can be qualified as joint controller for the initiation of the collection of newsletter reader behaviour data. See Section 5.3 below.

5.2 The role of Microsoft as data processor

Based on the privacy-amendment negotiated by SLM Rijk, Microsoft may only process the personal data in and about the use of the Azure AD in a role as data processor.

As a data processor, Microsoft may only process the personal data for the agreed purposes mentioned in Section 4.1.

5.2.1 Azure AD authentication cookies and logs

As part of the online authentication in the Azure AD, Microsoft sets functional authentication cookies. Microsoft also makes audit logs available to the customer, and processes aggregated data as processor for software debugging. Processing for these purposes fits in the processor role of keeping the service secure.

To the extent Microsoft mentioned other purposes such as 'research' and 'user analysis' in earlier AD documentation, processing for such purposes is excluded in the framework agreement with the Dutch government.

Microsoft is permitted to further process anonymous data for auditing and system-wide analysis, as part of the agreed legitimate business purposes, but is contractually bound to comply with the EDPB definition of 'anonymisation'. See Section 5.3 for an explanation of these legitimate business purposes.

A government organisation that does not want to permit Microsoft to further process anonymised data for its own legitimate business purposes, can use the *on-premise* AD.

5.2.2 Effective audit rights

The Dutch government has negotiated effective audit rights in the privacy amendment. The amendment covers Microsoft's obligation to ensure cooperation, including the relevant subprocessors, to provide all reasonable assistance in relation to all the audit activities of the controller.

5.2.3 Control over subprocessors

Microsoft provides a reference to a list of subprocessors in its terms and conditions.[54] Based on this list there is one subprocessor that could process the personal data in third countries: the US company Arkose Labs Inc. This company processes personal data for CAPTCA based fraud and abuse prevention activity related to the Azure AD.[55] In reply to this DPIA, Microsoft has explained that Enterprise and Education customers are never shown captchas, and hence, no personal data from Dutch government and Education customers are shared with this subprocessor.[56] Microsoft has also explained

[54].Microsoft General - Online Services Subprocessors List (2.7.23), last update 6 February 2023, URL: https://servicetrust.microsoft.com/DocumentPage/aead9e68-1190-4d90-ad93-36418de5c594

[55] Idem, listed as subprocessor that provides ancillary services.

[56] Conference call Microsoft, SLM Rijk and Privacy Company, 16 August 2023.

that if a service is offered in the EU Data Boundary, no data are ever shared with subprocessors outside of the EU.[57]

5.2.4 *Retention periods*

The only relevant retention periods Microsoft predetermines as a data processor in the tested setup are for the tracking pixel and for the Azure authentication data. Government organisations are in control over these retention periods by applying the privacy controls in Sections 3.5, 3.6 and disabling the tracking pixel, and by deleting data from former employees from the Azure AD.

5.3 The role of Microsoft as joint data controller

The European Court of Justice has clarified in three rulings[58] that parties may easily be qualified as joint controllers. This also applies when they do not have access to all the data collected by the other party, or when the levels of responsibility are very unevenly divided.[59] While the three rulings originate in disputes about the European Data Protection Directive, the definition of joint controller did not materially change in the GDPR. The GDPR only adds extra obligations (in Article 26) for joint controllers to transparently determine their roles and responsibilities.

As explained in Section 2.6.4 Microsoft by default uses a *tracking pixel* in newsletters sent with the Dynamics Marketing Module. With this pixel, Microsoft is able to present detailed reader statistics to its customers in the *on-premise* logs.[60]

If a government organisation does not disable the tracking pixel, the software automatically collects information about the recipient's interaction with the pixel, and presents analytics in a dashboard. As data controller for the *on premise* Dynamics Microsoft has decided to initiate this data processing. Even if Microsoft does not have access to the *on premise* dashboards, the data processing in dashboards is inextricably linked to the design of the software. Microsoft has also decided that individual opt-outs from the tracking of the reading behaviour only result in anonymisation of the information.

The French supervisory authority CNIL recently fined the French advertising network Criteo for not being able to demonstrate as joint controller with its customers that consent was obtained for the processing of personal data through tracking cookies.

---

[57] Idem.

[58] European Court of Justice, C-40/17, 29 July 2019, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629, C210/16, 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein versus Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388. See in particular par. 38-43. Also see: C-25/17, 10 July 2018, Tietosuojavaltuutettu versus Jehovah's Witnesses — Religious Community, ECLI:EU:C:2018:551, par. 66-69.

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

[60] Microsoft, Email marketing analytics report for Dynamics 365 Marketing, 1 August 2023, URL: https://learn.microsoft.com/en-us/dynamics365/marketing/marketing-analytics/analytics-gallery-email#interaction-timeline.

The CNIL said that the warning Criteo used, that its customers were exclusively responsible for obtaining the necessary consent, was not sufficient.[61]

This ruling illustrates that Microsoft may well be qualified as joint controller with the government organisation for the collection of tracking data through pixels, since Microsoft uses the same type of warning, without being able to verify if the individual recipient has consented to the tracking pixel.

5.4 The role of Microsoft as (independent) data controller

If Microsoft processes some personal data from its customers for its own legitimate business purposes, it acts as an independent data controller. This is the case when Microsoft is processing contact details of representatives of the customer for the conclusion of contracts and for billing purposes.

Additionally, Microsoft is permitted to further process some personal data, when necessary, for its own legitimate purposes as data controller. See Section 4.2 of this report. One of these purposes is compelled disclosure of personal data to a government authority. If law enforcement would compel Microsoft in its role as processor for the personal data from Enterprise customers to disclose Customer Data, Microsoft commits to try to redirect the request to the customer (the data controller), and only disclose data directly to law enforcement agencies when compelled to do so. In these cases, Microsoft commits to notifying the customer promptly of the access.[62]

Microsoft makes strong promises to principally challenge each such order and to pay compensation to each data subject affected by such a disclosure of Customer Data. Microsoft's VP for privacy, former FTC commissioner Julie Brill, explains in an official blog post:[63]

> *"First, we are committing that we will challenge every government request for public sector or enterprise Customer Data – from any government – where there is a lawful basis for doing so. This strong commitment goes beyond the proposed recommendations of the EDPB.*
>
> *Second, we will provide monetary compensation to these customers' users if we disclose their data in response to a government request in violation of the EU's General Data Protection Regulation (GDPR). This commitment also exceeds the EDPB's recommendations. It shows Microsoft is confident that we will protect our public sector and enterprise customers' data and not expose it to inappropriate disclosure."*

Microsoft twice per year publishes a detailed transparency report about the amount of law enforcement requests it has received[64], and a separate report with an

---

[61] CNIL, Personalised advertising: CRITEO fined EUR 40 million, 22 June 2023, URL: https://www.cnil.fr/en/personalised-advertising-criteo-fined-eur-40-million.

[62] Ibid.

[63] Blog Julie Brill, New Steps to Defend Your Data, 19 November 2020, URL: https://blogs.microsoft.com/onthe-issues/2020/11/19/defending-your-data-edpb-gdpr/

[64] Microsoft, How many enterprise cloud customers are impacted by law enforcement requests? URL: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

aggregate number of requests under U.S. national security laws, such as the Foreign Intelligence Surveillance Act (FISA).[65]

Microsoft has published in November 2021 that it has **never** disclosed personal data from any EU public sector customer to any government.[66]

Even though Microsoft has publicly raised alarm about the increasing number of gagging orders , in practice, this risk apparently has not materialised for the Dutch government. Microsoft clearly explains that it will disclose the number of orders received, regardless of a gagging order.

5.5 The role of other third parties

In the tested setup, an external supplier was involved, a party hired to implement the *on-premise* Dynamics 365. This external supplier was also engaged to provide maintenance of the system after its development, which can include some processing (viewing) of personal data. This data processing is out of scope of this umbrella DPIA, but government organisations are advised to assess the role of the supplier and mitigate possible data protection risks resulting from access to personal data by this supplier.

6. Interests in the data processing

This section outlines the different interests of Microsoft and of the Dutch government, but this section does not describe the fundamental data protection rights and interests of employees as data subjects. How their rights relate to the interests of Microsoft and the Dutch government organisations will be analysed in part B of this DPIA.

6.1 Interests Dutch government organisations

Dutch government organisations have security, efficiency and compliance reasons to use a centralised CRM platform. The *on-premise* Dynamics 365 provides such a service. Like all other organisations, government organisations also have a strong general interest in providing reliable, always on, well integrated and location independent administration tools to their employees. With the help of the Azure AD the server can also be reached from external locations, so employees can work from home or on the road.

The Dutch government has a geopolitical interest in storing data in local data centres or, alternatively, in a limited number of data centres in the EU. According to a recent news article as many as nine-tenths of Microsoft's Dynamics customers are still running the software on premises, in stead of using Microsoft's cloud services.[67]

The Dutch government must also comply with GDPR and ePrivacy rules. The ability to exclude sensitive data from the Audit tables, as well as the options to disable tracking

---

[65] Microsoft, U.S. National Security Orders Reports online summary, URL: https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1%3aprimaryr2

[66] Microsoft, Compliance with EU transfer requirements for personal data in the Microsoft cloud, November 2021, URL: https://go.microsoft.com/fwlink/p/?LinkID=2184913 .

[67] CIO, Microsoft offers Dynamics users fresh incentives to move to the cloud, 18 July 2023, URL: https://www.cio.com/article/646580/microsoft-offers-dynamics-users-fresh-incentives-to-move-to-the-cloud.html. The article quotes Hyoun Park, chief analyst at Amalgam Insights: "*Microsoft has almost 200,000 customers across CRM and ERP, but Dynamics 365 on cloud currently has about 20,000 customers.*"

tools in marketing module are essential in that regard. Additionally, the Dutch government needs to be able to remove data from former employees.

The Dutch government has a strong security interest in being able to access log data about user behaviour through audit logs, to comply with obligations as data controller to regularly inspect the files for unauthorised access to personal data. The Audit tables and logs files are essential to detect possible data breaches, and determine their scope. Through the Content Search on the diagnostic log files, system administrators can access data about users' access to personal data.

6.2 Interests Microsoft

Microsoft has wanted to be cloud first and mobile first since 2014. Microsoft explains:

> *"Our users don't simply use a workstation at a desk to do their jobs anymore. They're using their phone, their tablet, their laptop, and their desktop computer, if they have one. It's evolved into a devices ecosystem rather than a single productivity device* (…)*."*[68]

Microsoft has explained that it competes with other large-scale cloud providers and considers it an essential economic interest to be able to process large amounts of data to develop new services.

> *"But this [the switch to Office 365 cloud-only service] also brings enormous benefits. We already provide many intelligent services, combined with a service component. There is no question that we will analyse patterns and practices not only to improve security, but also to investigate whether there are new tools we want to build, also based on competitors, and questions from customers. This has to be possible. We will use data to the max, within what the law allows us."*[69]

Microsoft has a strong financial and economic interest in selling customers a monthly cloud-based subscription service, in stead of selling server software. Though Microsoft still provides Dynamics as *on-premise* software, new versions come packaged with other online services, most recently with the AI Copilot. The vision of Microsoft is cloud-first, and pricing schemes strongly encourage the Dutch government to switch from *on-premise* deployments to cloud only services. Microsoft is effectively putting pressure on institutions to switch to the monthly model because it will end its support for older versions in January 2027.[70]

Microsoft has strong business ethical interests to comply with international privacy and security standards and laws. In a world where many government organisations are still hesitant to entrust personal data to a cloud service provider, Microsoft puts strong efforts in providing online services that are compliant with the GDPR and compliant with globally acknowledged security standards. In May 2021, Microsoft's President Brad Smith announced that Microsoft is creating EU Data Boundaries, to allow organisations in the EU to exclusively process all data (from Core Online

---

[68] Microsoft blog, Cloud-first, mobile-first: Microsoft moves to a fully wireless network, August 17, 2016, URL: https://azure.microsoft.com/nl-nl/blog/cloud-first-mobile-first-microsoft-moves-to-a-fully-wireless-network/

[69] Microsoft Office 365 DPIA, Meeting report 30 August 2018, answer to Q46.

[70] Microsoft, Support extended for Dynamics 365 for Customer Engagement Apps, v9 (on-premises), URL: https://learn.microsoft.com/en-us/lifecycle/announcements/dynamics-365-customer-engagement-apps-v9-support-extended

Services) in data centres in the EU.[71] Though the implementation was announced to be completed by the end of 2022[72], Microsoft quietly backtracked on this promise, and announced it would start the phased roll-out per 1 January 2023.[73] According to its most recent updates, some work won't be completed until the end of 2024, for example with regard to Support Data.[74]

Microsoft has a strong track record in fighting disclosure of personal data for law enforcement purposes. Microsoft is the only major cloud provider that promises to legally challenge any order for personal data from its (Enterprise) customers, if it is not allowed to forward the request to its customer, and pay a financial compensation if it is compelled to disclose personal data.

6.3 Joint interests

The interests of Microsoft and the Dutch public sector organisations align when it comes to the use of Account and Diagnostic Data to offer a secure authentication service for the *on-premise* server, to enable employees to also work from home. Microsoft's EU data localisation for its EU Enterprise customers certainly aligns with the interest of government organisations to use a public cloud service without transfer risks. The interests may not align when it comes to the dominant business model of cloud services, in stead of server software that can be deployed locally.

7. Transfer of personal data outside of the EEA

This section describes the possible transfers of personal data to countries outside of the European Economic Area (EEA), with the applicable rules and requirements.

7.1 Factual data transfers in the test set-up

In the test setup, there only potential data transfers related to the (cloud service) Azure AD, and to the legacy Dynamics server telemetry data. This Section assumes government organisations will block this Telemetry data stream, as the data are not required and no longer used by Microsoft.

If a government organisation uses for example Azure cloud hosting to store audit logs from the *on-premise* server, Microsoft treats those data as Customer (Content) Data, and processes these data as data processor, within the EU Data Boundary.[75]

If organisations want to prevent any transfer of (legible) personal data to the USA, they can use a local Active Directory. However, this section describes the transfer of personal data through the cloud Azure Active Directory in the test setup.

---

[71] Microsoft blog Brad Smith, Answering Europe's Call: Storing and Processing EU Data in the EU, 6 May 2021, URL: https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

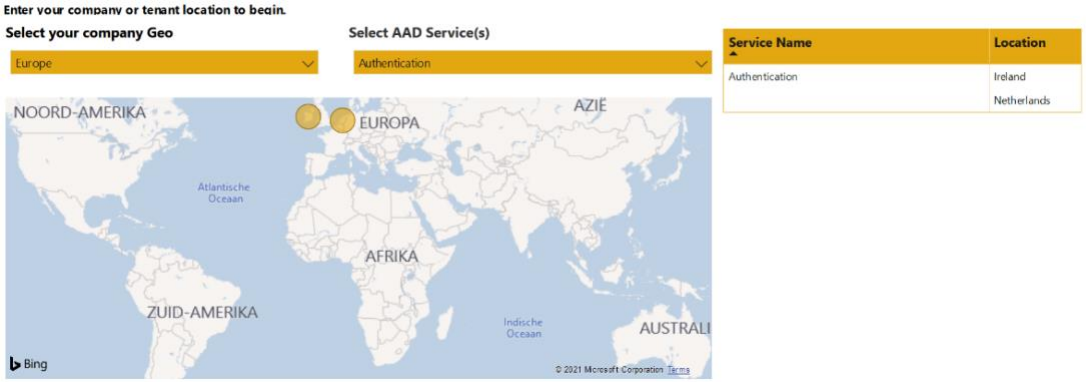
[72] Microsoft VP Julie Brill, EU Data Boundary for the Microsoft Cloud: A progress report 16 December 2021, URL: https://blogs.microsoft.com/eupolicy/2021/12/16/eu-data-boundary-for-the-microsoft-cloud-a-progress-report/

[73] Microsoft VP Julie Brill, Microsoft announces the phased rollout of the EU Data Boundary for the Microsoft Cloud begins January 1, 2023, 15 December 2022, URL: https://blogs.microsoft.com/eupolicy/2022/12/15/eu-data-boundary-cloud-rollout/

[74]

[75] Microsoft, On-premises software and client applications, 18 July 2023, URL: https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services.

Figure 21: Image of geolocation of processing data about authentication[76]



Enterprise Customers in the EU can select the geolocation where they want the Azure AD personal data to be stored. Microsoft offers a web page with an overview of the countries and data centres in which it offers the Azure services.[77] This shows that all Core Azure services, including the authentication data from the Azure Active Directory, can be stored in Western Europe (data at rest). The geolocation map in **Error! Reference source not found.** above shows that Microsoft offers to host the Azure AD data in Ireland and the Netherlands.

As mentioned in Section 6.2 above, Microsoft is still working on completion of the EU Data Boundary, to offer all core data processing through online services exclusively from within the EU.

The Azure AD cloud services are not currently listed as EU Data Boundary Services in Microsoft's Privacy and Security Terms for Online Services.[78] The Azure AD is listed in the EU Data Boundary documentation as an Azure service that is subject to temporary exclusion from the EU Data Boundary.[79] Microsoft writes:

> *"Azure AD operates as a non-regional service. Most Azure AD customer data is currently stored and processed in the EU Data Boundary for customers that have tenants based in the EU Data Boundary. Work is also ongoing to rearchitect portions of Azure AD to store and process all customer data in the EU Data Boundary. For more information about the customer data that will transfer out of the EU Data Boundary, see Identity data storage for European Customers in Azure Active Directory."*

The audit logs created by the use of the Azure AD do not contain personal data such as usernames, phone numbers, or IP addresses. However, the UserObjectId identifies authentication attempts to users. These logs, and activity reports, are already stored

---

[76] Ibid., Microsoft Azure Active Directory – Where is your data located?
[77] Microsoft geolocation overview for the Azure Core Services, URL: https://azure.microsoft.com/en-us/global-infrastructure/regions/#services.
[78] Microsoft licensing, privacy and security terms, URL: https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all.
[79] Microsoft, Services temporarily excluded from the EU Data Boundary, 19 July 2023, URL: https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-temporary-transfers-from-services#azure-services.

in the customer region[80], as well as push notifications from the Microsoft Authenticator app.

The only three exceptions are:

- "Multifactor authentication SMS and phone calls originate from datacenters in the customer's region and are routed by global providers. Phone calls using custom greetings always originate from data centers in the United States.
- General purpose user authentication requests from other regions are currently processed based on the user's location.
- Push notifications that use the Microsoft Authenticator app are currently processed in regional datacenters based on the user's location. Vendor-specific device services, such as Apple Push Notification Service or Google Firebase Cloud Messaging, might be outside the user's location."[81]
-

Microsoft also explains that it still processes some analytics on user and device account data, usage data and service configuration in the US, though Microsoft had planned to perform this processing within the EU Data Boundary by 1 January 2023.[82] Microsoft is working on migrating this processing to the EU, if the customer selects the location from the predefined list of processing regions for the EU.

Finally, Microsoft mentions it may replicate the AD data from EU customers outside of the EU Data Boundary. It is not clear why this is necessary, or if there are any means for customers to prevent this replication. It may well be related to enable authentication by traveling employees outside of the EU, as mentioned in the second bullet point above.

> "*EU Data Boundary Services may replicate directory data outside the EU Data Boundary from Azure Active Directory, including username and email address, to enable authentication into an EU Data Boundary Service and to obtain permissions for accessing data within an EU Data Boundary Service.*"[83]

7.2 (Sub-)processors outside of the EU

Microsoft only mentions 1 relevant subprocessor for the Azure AD, Arkose Labs Inc. for CAPTCA based fraud and abuse prevention activity related to the Azure AD. Arkose labs his headquartered in the USA, but may also process the data in Australia, Ireland and Singapore. As explained in Section 5.2.3, Microsoft does not use captchas with Enterprise and Education customers. Hence there are no transfer risks for Dutch government customers related to Microsoft's relation with subprocessor Arkose Inc for the Azure AD.

7.3 GDPR rules for transfers of personal data

The GDPR contains specific rules for the transfer of personal data to countries outside the EEA. In principle, personal data may only be transferred to countries outside the EEA if the country has an adequate level of protection. That level can be determined in a number of ways: a multinational may adopt Binding Corporate Rules, apply the

---

[80] See the Azure AD data location map at https://msit.powerbi.com/view?r=eyJrIjoiYzEyZTc5OTgtNTdlZS00ZTVkLWExN2ItOTM0OWU4NjljOGVjIiwidCI6IjcyZjk4OGJmLTg2ZjEtNDFhZi05MWFiLTJkN2NkMDExZGI0NyIsImMiOjV9

[81] Microsoft, Data residency and customer data for Azure Multi-Factor Authentication, 30 January 2023, URL: https://learn.microsoft.com/en-gb/azure/active-directory/authentication/concept-mfa-data-residency

[82] Idem.

[83] Idem.

EU Standard Contractual Clauses (SCC) or only transfer to countries for which the European Commission has taken a so-called adequacy decision.

7.3.1 Standard Contractual Clauses

Personal data may be transferred from the EEA to third countries outside of the EEA using Standard Contractual Clauses (SCC, also known as EU model clauses) adopted by the European Commission.[84] These clauses (hereinafter: SCC) contractually ensure a high level of protection. Microsoft will continue to offer the (new 2021) SCC to its Enterprise customers to legitimise the transfer of personal (Diagnostic, Account and Support) data from its EU customers to the USA.

7.3.2 European Commission Adequacy decision for the USA

An adequacy decision means that the country in question has a level of protection comparable to that applied within the EEA. Currently, there are adequacy decisions with respect to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the UK, Uruguay and for the USA.[85]

On 10 July 2023, the European Commission issued a renewed adequacy decision for the USA.[86] As a result, the US no longer counts as a *third country*, and European organisations are allowed to transfer personal data to US based cloud service providers without any additional protective measures, provided that the importing organisations have registered themselves for these specific services, as a participant in the Data Privacy Framework. Microsoft is registered as an active participant, but only for consumer services, which are covered by the general Privacy Statement.[87]

History of the new adequacy decision

On 16 July 2020, the European Court of Justice ruled that the adequacy decision for the USA based on the EU US Privacy Shield was no longer valid, with immediate effect.[88] This Schrems II judgment was the outcome of the lawsuit Max Schrems conducted against Facebook Ireland and the Irish Data Protection Commissioner. Earlier, in 2015, in another case instigated by Max Schrems, the European Court ruled the Safe Harbor agreement invalid, the predecessor of the Privacy Shield.

It took two years of negotiations, but on 25 March 2022, President Joe Biden and European Commission President Ursula von der Leyen signed an agreement in principle to develop new legal measures to ensure adequate personal data protection for US businesses. On 7 October 2022, President Biden signed a new Executive Order

[84] Based on the Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/6794 June 2021, URL: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf

[85] European Commission, Adequacy decisions, URL last visited 31 August 2023: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[86] Press release European Commission, 10 July 2023, URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

[87] Data Privacy Framework program, registration Microsoft for HR and non-HR personal data, URL: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active.

[88] European Court of Justice, C-311/18, Data Protection Commissioner against Facebook Ireland Ltd and Maximillian Schrems (Schrems-II), 16 July 2020.

of the President (EOP) to implement the commitments in the new agreement, the Trans-Atlantic Data Privacy Framework.[89]

The EOP contains new binding safeguards for data collection by US intelligence agencies and a new appeals process. [90] Following this EOP, the European Commission prepared a new draft adequacy decision.[91] The Commission asked the EDPB for its opinion. The EDPB issued its opinion in February 2023. The EDPB appreciated the significant improvements offered by the EOP, but expressed concerns, asked for clarification and called on the Commission to monitor implementation in future joint reviews.[92]

The European Parliament's LIBE committee was much more critical, adopting an opinion on 13 April 2023 rejecting the draft adequacy decision and calling on the Commission to renegotiate with the US.[93] The EP majority also rejected the draft decision on 11 May 2023 , but only had an advisory, not decision-making role.[94] After the agreement of member state ministers (the Council), the Commission adopted the decision on 10 July 2023.

7.4 Data Transfer Impact Assessment

As explained above, according to the European Commission, the US has regained an adequate level of protection since July 2023. It follows from the public guidance from the European Commission and European data protection authorities (EDPB) that the new US privacy safeguards apply to all personal data transferred to the US. Therefore, government organisations may continue to rely on the Standard Contractual Clauses, for those transfers, as long as Microsoft is not listed as participant for its Enterprise services.

The EDPB writes:

> "(...) *the EDPB underlines that all the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transferred to the US, regardless of the transfer*

[89] European Commission press release, European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework, 25 March 2022, URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087

[90] Executive Order of the President, Enhancing Safeguards for United States Signals Intelligence Activities, URL: https://www.whitehouse.gov/briefing-room/presidentialactions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signalsintelligence-activities/ .

[91] Press release European Commission, Commercial sector: launch of the adoption procedure for a draft adequacy decision on the EU-U.S. Trans-Atlantic Data Privacy Framework, 12 December 2022, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

[92] EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Trans-Atlantic Data Privacy Framework, 28 February 2023, URL: https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf.

[93] European Parliament, MEPs against greenlighting personal data transfers with the U.S. under current rules, 13 April 2023, URL: https://www.europarl.europa.eu/news/en/press-room/20230411IPR79501/meps-against-greenlighting-data-transfers-with-the-u-s-under-current-rules.

[94] Resolution European Parliament adopted 11 May 2023, with 306 votes for, 27 against and 231 abstentions, URL: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html.

> *tool used. Therefore, when assessing the effectiveness of the Article 46 GDPR transfer tool chosen11, data exporters should take into account the assessment conducted by the Commission in the Adequacy Decision.*" [95]

Max Schrems has announced that he will challenge the Adequacy Decision again in the European Court of Justice.[96] If the ECJ rules in his favour for the third time, and the adequacy decision would again be invalidated, Dutch government organisations will have to carry out a DTIA, a Data Transfer Impact Assessment, because the US would then again become a *third country*. The SCC are then no longer sufficient, according to the European Court of Justice's explanation in Schrems II. In it, the Court recognises the validity of the SCC, but prescribes that the exporting organisations must examine the level of protection in the recipient country.

The EDPB's guidance on that risk assessment shows that controllers are allowed to assess if the relevant problematic laws in the recipient country are actually applied to the transferred data. SLM Rijk has already published a DTIA on the risks of transfer of personal data through Microsoft's Enterprise services Teams, OneDrive and SharePoint Online. This public DTIA shows that the data protection risks of the transfer of regular and pseudonymous personal data can already be assessed as extremely low, even without an adequacy decision. This is mainly because the extremely low likelihood of Microsoft being forced to provide personal data of its European public sector customers. Microsoft has publicly stated that it has never provided European public sector customer data to any government, i.e. including disclosures to US intelligence agencies. In doing so, Microsoft explained that it is legally prohibited from publishing the exact number of times it has *received* a demand/order from the intelligence agencies it has received, but thus not, how many times it has actually *provided* data.

The new EU US agreement does not change the powers from US law enforcement to compel disclosure of personal data from EU Enterprise customers under the US CLOUD Act (*Clarifying Lawful Overseas Use of Data*). This act was specifically designed to obtain access to data stored in data centres in the EU. This act extends the jurisdiction of North American courts to all data under the control of U.S. companies, even if those data are stored in data centres outside the territory of the United States.

As the European Parliament notes in its opinion on the Data Privacy Framework:

> "*the EO [Executive Order from the President, added by Privacy Company] does not apply to data accessed by public authorities via other means, for example through the US Cloud Act or the US Patriot Act, by commercial data purchases, or by voluntary data sharing agreements.*"[97].

---

[95] EDPB, Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023, URL: https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf.

[96] Noyb, "Privacy Shield 2.0"? - First Reaction by Max Schrems, 25 March 2022, URL: https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems.

[97] European Parliament LIBE committee opinion on the Data Privacy Framework, page 5 point 4, URL: https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf.

8. Additional legal obligations: ePrivacy Directive

In this paragraph, only the additional obligations arising from the ePrivacy Directive (ePD) are discussed. Given the limited scope of this DPIA, other legal obligations or policy rules (for example with regard to security), are not included in this report.

In the test setup users could only access the *on-premise* Dynamics 365 system through the (Microsoft Edge) browser on a Windows 10 device, not through mobile apps.

As described in Sections 2.6.4 and 2.6.7, Microsoft engages in two types of data processing that are subjected to the ePrivacy Directive rules: (i) the use of a tracking pixel in newsletters and (ii) the setting and reading of authentication cookies. These two types of data processing are described in separate sections below.

The act of reading or placing information (through cookies or similar technology), or enabling third parties to read information from the devices of end users triggers the applicability of Article 5(3) of the ePrivacy Directive, regardless of who places or reads the information, and regardless of whether the content is personal data or not. Consent is required prior to the retrieval or storage of information on the devices or browsers of end users, unless one of the exceptions applies, such as the necessity to deliver a requested service, or necessity for the technical transmission of information.

Based on article 3(1) of the GDPR, because the data processing takes place in the context of the activities of data controllers (Dutch government organisations), the GDPR applies to all phases of the processing of these data.

Applicability of the GDPR rules does not exclude applicability of the ePrivacy rules or vice versa. The European Data Protection Board writes:

"Case law of the Court of Justice of the European Union (CJEU) confirms that it is possible for processing to fall within the material scope of both the ePrivacy Directive and the GDPR at the same time. In Wirtschaftsakademie, the CJEU applied Directive 95/46/EC notwithstanding the fact that the underlying processing also involved processing operations falling into the material scope of the ePrivacy Directive. In the pending Fashion ID case, the Advocate General expressed the view that both set of rules may be applicable in a case involving social plug-ins and cookies.[98]

The consequences of the cookie provision are far-reaching, since it requires clear and complete information to be provided prior to the data processing, and it requires consent from the user, unless one of the legal exceptions applies. The consent is identical to the consent defined in the GDPR.

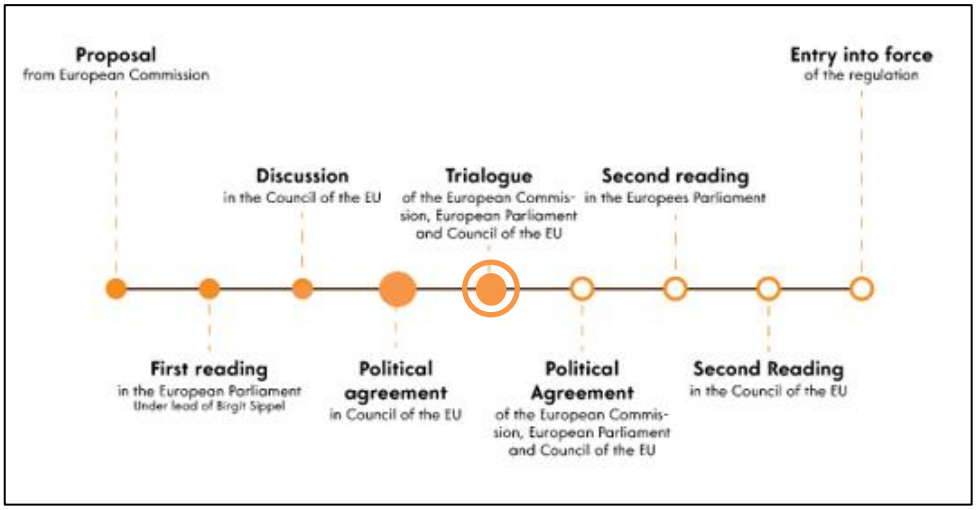
The most frequently used exception in the Netherlands is the processing of such information for analytical purposes, literally:

---

[98] EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, Paragraph 30. URL: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf In footnotes the EDPB refers to: CJEU, C-210/16, 5 June 2018, C-210/16, ECLI:EU:C:2018:388. See in particular paragraphs 33-34 and the Opinion of Advocate General Bobek in Fashion ID, C-40/17, 19 December 2018, ECLI:EU:C:2018:1039. See in particular paragraphs 111-115.

"to obtain information on the quality or effectiveness of a delivered information society service provided that it has no or little impact on the privacy of the subscriber or user concerned."

Figure 22: Timeline new ePrivacy Regulation



The consent requirement for tracking cookies will likely continue to exist in the future ePrivacy Regulation. On 10 January 2017, the European Commission published a proposal for a new ePrivacy Regulation.[99] This was followed by an intense political debate the last four years. The European Parliament responded quickly and positively, but it has taken the representatives of the EU Member States three years to draft a compromise about the proposed ePrivacy Regulation. The Council sent its agreed position to COREPER to start the trialogue on 10 February 2021.[100] The trilogues began on 20 May 2021. The last publicly available update from the Council dates from 28 March 2022, in which the proposed compromises are all blacked out.[101] Figure 22 above shows the required legislative steps for adoption of the ePrivacy Regulation.

The points of view of the European Parliament and the European Council are widely diverging. Therefore, it is not likely that the ePrivacy Regulation will enter into force anytime soon, and Microsoft will have to comply with the current ePrivacy rules in the next few years.

8.1 Tracking pixel

As described in Section 2.6.3, Microsoft includes a tracking pixel by default in the newsletters sent through *on-premise* Dynamics 365. Microsoft uses the pixel to provide analytics (Insights) to the customers of its Marketing Module. This enables them to see which directly identifiable customer/recipient opens the letter at what exact time, what links to articles he or she clicks on, and whether he/she forwards the newsletter.

---

[99] European Commission, Proposal for a Regulation on Privacy and Electronic Communications, 10.1.2017 COM(2017) 10 final, URL: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

[100] Council of the European Union, Interinstitutional File 2017/0003(COD), Brussels, 10 February 2021 (OR. en) 6087/21, URL: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

[101] French presidency, preparation for trialogue, 7458/22, 28 March 2022, URL: https://data.consilium.europa.eu/doc/document/ST-7458-2022-INIT/x/pdf.

If the government organisations do not turn off this pixel, based on Article 5 (3) ePD, they must first obtain the end-user consent before information is accessed that was stored on the user's device. In the test setup, the organisation did not ask for such prior consent, as Microsoft did not offer such a module. Microsoft also did not offer a 'disable' option to admins, nor an alternative solution, such as immediate anonymisation of all recipient personal data, and only providing statistics to the customer.

Based on article 5(3) of the ePrivacy Directive, the inclusion of the pixel is not necessary for carrying out or facilitating the transmission of a communication over an electronic communications network. Nor is the pixel strictly necessary in order to provide an information society service explicitly requested by the subscriber or user. Therefore, the customer has to obtain the informed, specific and freely given consent for the purpose of tracking the reading behaviour.

Microsoft did mention that customers had to ask for consent from their customers/recipients. But this advice from Microsoft was not sufficient for compliance, as consent is only valid if recipients can refuse the consent without adverse consequences, and if the recipient can withdraw the consent as easy as that the consent was given. This was not the case; recipients could only refuse by terminating their subscription to all newsletters sent by the government organisation. In practice, government organisations were thus forced to erect a tracking wall for the recipients of newsletters sent with Dynamics, to 'accept' the tracking or not receive the information.

In reply to this DPIA, Microsoft has provided options for Enterprise Dynamics 365 users to centrally disable the use of the tracking pixel for all subscribers, and to remove a similar tracking pixel from marketing forms used on a website. Microsoft distinguishes between realtime and outbound marketing. In the test setup only the outbound email marketing was used. Microsoft explains that customers can view and set the consent level for each contact

> "*Tracking: Choose whether to track contact interactions. If the box is set to Do Not Allow, Marketing won't track public interactions (email opening, email clicks). The tracking option allows contacts to specify whether they consent to having their interaction data saved. You can trigger this field by either adding the field to client consent forms or by updating the contact data directly.*"[102]

Microsoft recommends and facilitates the use of a self-service subscription center, where the relations can change their subscriptions, and give or revoke consent.[103]

Microsoft also warns that the auditing logs of such consent changes are by default disabled. Customers may want to keep a record of changes.

> "*The auditing system is usually disabled by default, so you need to set it up if you want to use it log your GDPR consent changes (and other information). When*

[102] Microsoft, Outbound marketing compliance settings, 7 July 2023, URL: https://learn.microsoft.com/en-us/dynamics365/marketing/privacy-use-features

[103] Idem, URL: https://learn.microsoft.com/en-us/dynamics365/marketing/privacy-use-features#include-a-consent-selector-in-a-subscription-center.

setting up the system, you are able to choose which types of events you want to audit on which type of records."[104]

8.2 Authentication cookies

Microsoft sets cookies when an employee logs-in to the Dynamics server through the browser. As described in Section 2.6.7, these cookies contain unique identifiers. Since the cookies are necessary to authenticate the user, and do not contain any additional or excessive tracking data, they can be qualified as functional cookies to transmit the authentication request. Therefore, consent from the employees is not required.

9. Retention Periods

Microsoft has assured SLM Rijk that it does not retain the legacy server Telemetry Data. The data are discarded immediately, as Microsoft has no use for these data. With the new policy provided in Annex 1, customers can and should disable this traffic.

Microsoft makes information available about the default retention periods of the Azure AD Account and Diagnostic Data.

Depending on the type of subscription (Free, Premium P1 or Premium P2), the logs from sign-ins, audit and provisioning are stored between 7 and 30 days. Customers can extend this retention period by routing the data to an Azure storage account.[105]

Figure 23: Microsoft table with Azure AD audit log retention periods

How long does Azure AD store the data?

Activity reports

Report	Azure AD Free	Azure AD Premium P1	Azure AD Premium P2
Audit logs	Seven days	30 days	30 days
Sign-ins	Seven days	30 days	30 days
Azure AD MFA usage	30 days	30 days	30 days

As noted in Section 3.2, admins can delete individual Diagnostic Data. Microsoft also enables admins to clean up old logs: "*You can delete the old or unwanted logs to clean up the database space. (...) You can only delete the oldest audit log in the system. To delete more than one audit log, continue to delete the oldest audit log until you have deleted enough logs.*"[106]

Microsoft also informs customers how long it retains security signals related to the Azure AD.

---

[104] Idem, URL: https://learn.microsoft.com/en-us/dynamics365/marketing/privacy-use-features#enable-auditing-to-log-all-record-changes

[105] Azure Active Directory data retention, 14 July 2023, URL: https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention.

[106] Microsoft, Recover database space by deleting audit logs, 15 June 2022, URL: https://learn.microsoft.com/en-us/power-platform/admin/recover-database-space-deleting-audit-logs

Figure 24: Retention periods security signals

Security signals

Report	Azure AD Free	Azure AD Premium P1	Azure AD Premium P2
Risky users	No limit	No limit	No limit
Risky sign-ins	7 days	30 days	90 days

ⓘ Note

Risky users and workload identities are not deleted until the risk has been remediated.

Part B. Lawfulness of the data processing

This second part of the DPIA assesses the lawfulness of the data processing. This part contains a discussion of the legal grounds, an assessment of the necessity and proportionality of the processing, and of the compatibility of the processing in relation to the purposes.

10. Legal Grounds

Any processing of personal data has to be based on a specific legal ground, as specified in Article 6(1) GDPR.

Essentially, for processing to be lawful, this article demands that the data controller bases the processing on the consent of the user, or on a legally defined necessity to process the personal data.

The grounds mentioned in Article 6(1) GDPR are as follows:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

c) processing is necessary for compliance with a legal obligation to which the controller is subjected.

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person.

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

This section first describes the legal ground when the government organisation is the data controller, and Microsoft is the data processor. The second section describes data processing by Microsoft as controller for the authorised further processing purposes.

To determine whether a legal ground is available for a specific processing operation, it is necessary to determine for what purpose, or what purposes, the data are collected and will be (further) processed. There must be a legal ground for each of these purposes. As data processor for the Azure AD data Microsoft may only process the personal data for the three agreed purposes.

The first section only mentions five of the six different possible legal grounds for the processing of the Account, Content and Diagnostic Data by government organisations. The legal ground of vital interest is not discussed, since nor Microsoft nor Dutch government organisations have a vital (lifesaving) interest in processing personal data via Dynamics or the Azure AD.

10.1 Consent

Article 6 (1) (a) GDPR reads: "*the data subject has given consent to the processing of his or her personal data for one or more specific purposes*". If a data subject has freely given consent for the processing, such consent can be the legal ground for the processing of the data. This ground requires that the consent was freely given, after the data subject has been informed about the scope and potential risks associated with the processing. It also requires that the data subject is able to withdraw the consent without negative consequences.

In the test set-up of the *on-premise* Dynamics 365 implementation consent was required for subscriptions to newsletters. Explicit consent (the exception on the prohibition on the processing of special categories of data)was required for the storing of self-provided information about dietary requirements and allergies. These consents were obtained from data subjects in a separate way, not through the *on-premise* Dynamics 365 system. In the test set-up, there was no Do It Yourself digital dashboard to help data subjects exercise their rights digitally, such as withdrawal of their consent, or removal of sensitive data. Removals were handled by admins.

In its role as controller for a limited list of legitimate business purposes, Microsoft is not allowed and does not rely on consent from employees for the processing of Diagnostic Data. Given their dependence on their employer employees may not feel free to refuse such consent. Consent is therefore not a valid legal ground for Microsoft for the processing of Diagnostic Data.

The ePrivacy Directive (ePD) requires consent for subscriptions to newsletters, and for adding and reading a tracking pixel in a newsletter. Such data processing does not qualify as necessary. Government organisations must therefore obtain the prior consent of recipients for both the newsletter, and for the purpose of tracking the way recipients read the newsletter. This reasoning was confirmed by the Danish DPA, in a public reprimand of an organisation for the use of a tracking pixel in newsletters without properly informing the recipients, and without obtaining their consent.[107] Alternatively, government organisations can instruct Microsoft to turn off the tracking pixel. Other legal grounds of the processing are not relevant for this processing, since the ePD requires consent.

10.2 Processing is necessary for the performance of a contract

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

Government employees are provided with a Dynamics account to be able to carry out the tasks included in their job description. Based on the framework contract with the Dutch government, Microsoft may only process the limited personal data it receives from the on premise server and the Azure AD for the three purposes identified in Section 4.1. Therefore, government organisations may successfully rely on the legal ground of necessity for a contract if the processing of the Diagnostic Data from these services is strictly necessary for the performance of the employment contract between the data subject and the government organisation.

---

[107] Danish DPA, reprimand for the use of spy pixel, in Danish only, February 2023, URL: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/feb/anvendelse-af-spy-pixels-i-forbindelse-med-udsendelse-af-nyhedsbrev.

This legal ground, however, is only applicable insofar as Microsoft qualifies as processor for the Dutch government organisation. Microsoft itself does not have a contract with the data subjects, and therefore cannot itself rely on this legal ground as a controller for any part of the processing. Even if checking a box to use a service or downloading an app without any information about the consequences in terms of personal data processing could possibly qualify in civil law as an intention to conclude an agreement, such processing does not meet the requirements of the legal ground of Article 6(1)(b) of the GDPR: the necessity to process specific personal data to perform a specific contract with each specific data subject.

In view of the explanation of Microsoft that the server Telemetry Data from server installs prior to 2018 are obsolete, and immediately discarded, there clearly is no necessity for either Microsoft to continue to collect these data, or for government organisations to continue to send them. In reply to this DPIA, Microsoft has provided policy rules to enable government organisations to block this data stream. See Annex 1.

10.3 Processing is necessary to comply with a legal obligation

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

This legal ground can only be invoked for specific purposes if these purposes have been laid down in the law. The processing of personal data should follow directly from this law, or should be implicitly included. Though there is a general legal obligation in the GDPR to guarantee the security of personal data, the GDPR does not specify what personal data have to be processed for this security purpose. So, there is no specific legal obligation following from the GDPR to process Diagnostic Data or to retain (audit) log files for an extended period of time. However, Article 32(1)(d) of the GDPR obliges organisations to have a process for regularly assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. Organisations need to periodically review the log files to detect if any incidents or breaches have occurred.

The ICO explains: *"If you operate automated processing systems (any IT database), you must keep logs for at least the following processing actions:*

- *Collection*
- *Alteration*
- *Consultation*
- *Disclosure (including transfers)*
- *Combination*
- *Erasure"*[108]

It follows from Article 28 GDPR that data controllers may only use data processors that provide "sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

Even though logging is necessary, the legal security obligations in the GDPR are not specific enough for organisations to rely on this legal ground. However, they may only use data processors that can provide adequate logging to ensure the security of the data processing.

[108] ICO, logging, URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/logging/

10.4 Processing is necessary for a task in the public interest or for the legitimate interests of the controller or a third party

Article 6(1)(e) of the GDPR reads: "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".
Article 6(1)(f) of the GDPR reads as follows: "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

Dutch government organisations may perform public interests by processing personal data in the *on-premise* software. If they use the Dynamics software to maintain contact lists of relations and to organise events, including the registration of dietary preferences or allergies of invited attendees, it is unlikely they can rely on the legal ground of Article 6(1)e of the GDPR. The processing of personal data for these purposes in a Dynamics server is not strictly necessary for the performance of public tasks, even if such data processing does strengthen those public tasks.

Other government organisations may well be able to rely on this legal ground for the processing of Content Data through the *on-premise* Dynamics 365, depending on the information they process and the tasks in the public interest assigned to them. Processing of Diagnostic Data by Microsoft for its own legitimate business purposes is too far removed to be able to be justified on the basis of necessity to perform tasks in the public interest. There is no specific public interest served by using specific Microsoft services.

Government organisations can seldomly rely on the legal ground of necessity of the processing for their legitimate interest. As the last sentence of Article 6 (1) GDPR specifies, this legal ground shall not apply to processing carried out by public authorities in the performance of their tasks. Whether this includes all activities by public authorities remains to be determined in decisions from Data Protection Authorities or jurisprudence.

When government organisations do not perform a task in the public interest through the use of (specifically) *on-premise* Dynamics 365 as a database, but as part of their business operations, and consent is not an option, they must be able to rely on the necessity for their legitimate interest, both for the Content and for the Diagnostic Data processing in the audit logs, as the only available legal ground. This requires the organisation to clearly specify its legitimate interest and to weigh it against the rights and freedoms and the interests of the data subjects. If the rights, freedoms, or interests of the data subjects override the legitimate interests of the government organisation, the processing cannot be lawful.

The processing of personal data by Microsoft of Azure AD data as a processor falls within the scope of the legitimate interest of its Enterprise customers (here: the government organisations) as data controllers. Only if Microsoft processes personal data in a role as data controller, the legal ground of the legitimate interest of Microsoft needs to be separately considered and weighed against the rights, freedoms, and interests of the data subjects. To ensure prevalence of data subject rights, the framework contract specifies that Microsoft may only process personal data when proportionate, and only in identifiable format (in stead of aggregated or anonymised) when unavoidable in relation to the identified legitimate business purposes.

11. Special categories of personal data

The GDPR prohibits the processing of special categories of personal data, unless one of the exceptions listed in Article 9(2) of the GDPR applies. Depending on the way an organisation implements the *on-premise* Dynamics 365, it is possible that special categories of personal data are included in the processing, such as for example health related issues of visitors / participants. Such special categories of data can also appear in the Audit tables, if these data are not specifically excluded by the government organisation.

On what exception a government organisation can rely depends on the purposes for which the organisation collects and stores the information. For the exception to be valid, it has to be fully applicable, and all conditions have to be met. The government organisation has to be able to demonstrate that it meets these requirements. This is particularly relevant if a government organisation does not follow the recommendation to exclude special categories of data from the audit tables.

Of the available exceptions, there are only two relevant for generic CRM purposes: (1) explicit consent, or (2) the data subject has made the data public. If an organisation for example has as specific public task to process health data, other exceptions may be relevant.

In the test set-up, personal data from contact persons included the name of the organisation they work for. Such employer names can be revealing of the political or religious background of these contact persons, or possibly of other types of special categories of personal data.[109] A possible exception for this kind of data processing is the fact that data subjects have themselves made this information public, the exception in Article 9(2)(e) of the GDPR. However, this exception must be interpreted narrowly.

The ECJ ruled that the exception of the data having been made public could not be invoked by Meta: "where the user of an online social network visits websites or apps to which one or more of the categories set out in Article 9(1) of that regulation relate, the user does not manifestly make public, within the meaning of the first of those provisions, the data relating to those visits collected by the operator of that online social network via cookies or similar storage technologies;
Where he or she enters information into such websites or apps or where he or she clicks or taps on buttons integrated into those sites and apps, such as the 'Like' or 'Share' buttons or buttons (.... are only made public) where he or she has explicitly made the choice beforehand, as the case may be on the basis of individual settings selected with full knowledge of the facts, to make the data relating to him or her publicly accessible to an unlimited number of persons;" [110]

The test set-up also included processing of information about diets and allergies of attendees of events, to provide people with the right meal. Since dietary requirements can reveal information about religion or health, and allergy information is always

[109] In C-184/20 from 1 August 2022, ECLI:EU:C:2022:601, the European Court of Justice found that the processing of any personal data that are "*liable indirectly to reveal sensitive information concerning a natural person*", i.e. any information that may reveal a person's racial or ethnic origin, religious or philosophical beliefs, political views, trade union membership, health status or sexual orientation, is subject to the prohibition from processing under Article 9(1) GDPR, unless an exception under Article 9(2) applies.

[110] Case C-252/21 (Meta vs the German competition authority) from 4 July 2023, ECLI:EU:C:2023:537, par. 73.

about health, these data types fall under the prohibition of the processing of special categories of data.

Government organisations must ensure they obtain explicit consent from data subjects to process this information. They must also ensure that they restrict access to these fields based on a need-to-know basis, and limit the retention period to the minimum necessary.

The storage of the dietary and allergy information in the audit tables for security purposes can be considered legitimate if the primary processing is legitimate. Storage of these data after the expiration of the retention period is not legitimate.

12. Purpose limitation

Article 5 (1) (b) GDPR obliges data controllers to comply with the principle of purpose limitation. Data may only be

"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes."

Essentially, this means that the controller must have a specified purpose for which he collects personal data and can only process these data for purposes compatible with that original purpose, unless the controller can meet additional requirements, that must be met before any further processing can take place.

12.1.1 Purposes for Dutch government organisations

As described in Section 4.1, in the test set-up 11 purposes were identified for the processing of personal data in scope of this DPIA, six related to the processing of personal data from external data subjects, and five related to the processing of employee data.

Purposes external data subjects	Purposes employee data
1. Relationship management, entry, updating and manual deletion of contact information	7. Administration of the system, including setting up roles for specific users and their permissions.
2. Verification of the address data in the CRM system, through the use of an external online service.	8. Authentication and authorisation of employees with the Azure AD.
3. Creating back-ups of the database.	9. Logging of changes made to specific records (with the Audit tables).
4. Organisation of meetings and events, segmentation of contacts and sending of letters and (e-)mail(ing)s.	10. General security purposes (detection of unlawful access and data breaches with the technical logs and the Audit tables, back-ups of the database).
5. Remembering food preferences: dietary preferences of relations visiting customer organised events.	11. Removal of obsolete personal data from the Audit tables (individually or by date range).
6. Tracking of newsletter reading with pixels.	

Based on article 6(4) of the GDPR, the controller must take at least 5 criteria into account to test the compatibility of the further processing of personal data for a related purpose.

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing.
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller.
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10.
(d) the possible consequences of the intended further processing for data subjects.
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."

The link (a) between purposes 1, 3 and 4 is clear: to manage the relationship between a government organisation and the data subjects. When data subjects provide their data to a government organisation, they should be informed that these data can be used to invite them to events and meetings. If they provide consent they can also expect to receive mailings.

There is a similar clear link between the processing of the contact data from external data subjects with the maintaining a back-up and the processing of employee data for technical employee management, even if those purposes are not explicitly mentioned during the collection of the data. The processing therefore makes sense within the context (b) of the relationship of the government organisation with the data subject.

However, there is no such clear link, or context, with processing for the purposes 2 (address verification) and 6 (tracking pixel). Verification of contact data by a third party could lead to a data breach, or to incorrect data, depending on the policy implemented by the organisation in case of differences, and the nature of the contract with the third party. If organisations do not follow the recommendation from this DPIA to disable the tracking pixel from the newsletter, and they do not obtain valid separate consent from the recipients, the processing is not compatible with the purpose of informing relations through a newsletter.

The personal data collected for the first, second and fifth purpose can include data of a sensitive nature (c), when the private contact details of prominent people are included, or when people provide health information about allergies or disabilities. To ensure compatibility of the further data processing, the government organisation must ensure it can rely on the explicit consent of those people, with a clear explanation of the purposes for which the data can be processed and a very short retention period.

With the exception of purposes 2 and 5, the possible consequences of the intended processing for the data subjects (d) are limited. No significant negative effects on their rights and freedoms are to be expected under normal operating conditions.

Government organisations can apply appropriate safeguards (e) to ensure compatibility of the processing for the first purpose by allowing people to flag the confidentiality of their contact data, by limiting the access to these specific data, and logging and verifying use of these data for the authorised purposes.

Government organisations should disable the tracking pixel (sixth purpose), and adopt a policy to prevent data breaches when they wish to use an external address verification service.

12.1.2 Purposes for which Microsoft processes personal data

Based on the enrolment framework, Microsoft is authorised to process personal data on behalf of the government organisation for three additional purposes. These are:

1. to provide and improve the service,
2. to keep the service up-to-date, and
3. to secure the service.

Microsoft can achieve these purposes for the Azure AD with the help of the Azure AD Diagnostic Data described in Section 2.6.3, and the cookies on the authentication website described in Section 2.6.7. Microsoft does not need to collect any personal data from the *on*-premise server.

13. Necessity and proportionality

Article 5(1)(c) of the GDPR requires that every processing is limited to what is necessary to achieve the set purpose(s). It is therefore important to examine whether every processing is in fact necessary for the purposes for which the data controllers process personal data.

The concept of necessity is made up of two related concepts: proportionality and subsidiarity. First it has to be assessed whether the same purpose can reasonably be achieved with other, less invasive means (subsidiarity). If so, these alternatives have to be used.

Second, proportionality demands a balancing act between the interests of the data subject and the data controller. The benefits of the processing for the data controller need to exceed the infringement it represents on the rights and freedoms of the data subjects. The processing should also not be excessive in relation to the purpose of the processing. If the purpose can be achieved by processing fewer personal data, then the amount of personal data processed should be decreased to what is necessary. Therefore, essentially, the data controller may process personal data insofar as is necessary to achieve the purpose, but may not process personal data he or she may do without. The application of the principle of proportionality is thus closely related to the principles of data protection from Article 5 GDPR.

13.1 Assessment of the subsidiarity

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

In the test set-up the government organisation processed personal data for 11 different purposes. As analysed in Section 12.1.1, most of these purposes were compatible with the main two purposes of processing data from external data subjects for customer relationship management, and processing of employee data for authentication and security purposes.

To organise meetings and invite contacts, and to send mailings, government organisations necessarily have to process contact data. The use of these data is recorded in the Audit tables. These logs can include data from deleted contacts, to ensure government organisations can restore data if they were mistakenly deleted.

The Content Data may include sensitive or special categories of data, relating to for example special needs or dietary allergies. In reply to this DPIA, Microsoft has pointed to guidance for admins how to stop recording and delete specific Content Data from

the Audit tables.[111] Since there are no compelling reasons to keep on processing special categories of data after a data subject has withdrawn consent, this finetuning of the audit logs is essential for government organisations to comply with the subsidiarity principle.

To ensure compliance with the data minimisation principle, organisations are also advised to develop a portal with Do It Yourself access to the data stored in the CRM, as well as allow for self-management of subscriptions to mailings.

Another element of the subsidiarity test is an assessment if alternative software vendors offer a service that achieves the same purposes with lesser risks for the data subjects. CRM products are widely available, many developed specifically for enterprise-level organisations, with hundreds or thousands of employees. Microsoft has many direct competitors for this product. However, realistic alternatives often come with the same or similar processings and involve similar or higher risks to the rights and freedoms of the data subjects. From the perspective of government organisations, there are no apparent alternatives that are materially better at the protection of the rights and freedoms of the data subjects.

13.2 Assessment of the proportionality

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

To assess whether the processing is proportionate to the interest pursued by the data controller(s), the processing must first meet the principles of Article 5 of the GDPR. As legal conditions they have to be complied with in order to make the data protection legitimate.[112]

Data must be '*processed lawfully, fairly and in a transparent manner in relation to the data subject*' (Article 5(1)(a) of the GDPR). This means that data subjects must be informed about the processing of their data, that all the legal conditions for data processing are adhered to, and that the principle of proportionality is respected.

Microsoft provides detailed information about its data collection related to the *on-premise* and cloud audit logs from the Dynamics server, and the Azure AD. Microsoft does not publish any information about the obsolete Telemetry Data. Since Microsoft has provided a policy in reply to this DPIA for admins to block the sending of these Telemetry Data, the lack of transparency does not make the Diagnostic Data processing inherently disproportionate.

---

[111] Microsoft, Enable or disable entities and fields for auditing, 16 February 2022, URL: https://learn.microsoft.com/en-us/dynamics365/customerengagement/*on-premise*s/admin/audit-data-user-activity?view=op-9-1#enable-or-disable-entities-and-fields-for-auditing.

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

Similarly, there is very little public information about the exact data processing with the tracking pixel. As described in Section 2.6.4, the analytics about the reading behaviour are unreliable. That means that even if the creation of analytics can be a legitimate purpose, this purpose cannot be achieved with the chosen means. In fact, the use of an invisible tracking pixel in the mail that allows for tracking of the recipient's behaviour infringes on the fundamental right to communications' secrecy. If a recipient has not been clearly informed about this practice, and was not able to freely consent to this infringement, the tracking with the pixel cannot be legitimate.

In reply to this DPIA Microsoft has provided an option for its customers to disable the pixel, to overcome this lack of fairness and transparency.

As analysed in Section 11, fair and lawful processing of special categories of data (such as dietary requirements) requires extra safeguards. Data subjects must be informed in an unambiguous way how the organisation will use these self-provided data and how long they will be retained. Additionally, organisations must make it as easy as possible for data subjects to withdraw this consent, preferably via a digital Do It Yourself access portal.

Some regular contact data in the database may be sensitive if they relate to people that have reasons to fear abuse, such as prominent people, people that are stalked, or employees that need to keep the identity of their employer confidential. To minimise the risks of unauthorised access to these data, organisations are advised to implement a 'warning' flag for such records, and implement limited access policies, and systematic log controls, accordingly. Such flagged data should not be exchanged with external verification services either.

By default Microsoft retains data in logs about the activity of changing or deleting records with personal data. This data processing is important for the purpose of maintaining the integrity and in order for organisations to repair mistakes. But this security logging conflicts to some degree with the requirement to irreversibly delete data after they are no longer necessary for the purpose for which it was collected.

The ICO explains: "*It is important that you do not record the data itself in your logs of erasure, as there is no need to retain a duplicate record of what you have erased. The requirement is to produce metadata which displays, for example, what a specific person on a specific date erased. The 'what' does not have to detail the content of the record/information that has been deleted – it can simply record that record* X *was updated by a specific individual*."[113]

In reply to this DPIA Microsoft has provided guidance for organisations to stop logging certain fields, and remove fields from logs.

The principles of data minimisation and privacy by default demand that the processing of personal data is limited to what is necessary: Data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (article 5 (1) (c) GDPR). This means that government organisations may not collect and store data (or allow Microsoft to collect and store data) which are not directly related to a legitimate purpose. According to this principle, the default settings for the data collection should be set in such a way as to minimise data collection by using the most privacy friendly settings. Microsoft complies with this principle in three ways:

---

[113] ICO, Logging, In brief, URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/logging/

1. by only setting necessary authentication cookies on the login page for the AD
2. by not using the Captcha service from a subprocessor in third countries.
3. by offering tools to admins to stop recording and delete unnecessary data from audit tables

Unfortunately, Microsoft does not comply with the privacy by default requirement with regard to the newsletters: the tracking pixel is by default enabled, and admins must take steps to disable this processing, or obtain separate consent from the recipients.

The principle of storage limitation demands that personal data are only retained as long as necessary for the purpose in question. Data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*" (article 5(1)(e), first sentence of the GDPR). This principle therefore demands that personal data are deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller. The text of this provision goes on to clarify that "*personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject*" (article 5(1)(e), second sentence, of the GDPR).

As described in Section 9 of this report, Microsoft publishes detailed information about the different retention periods for the logs. These periods are short. Admins can decide to export the logs and determine longer retention periods.
In view of the strict purpose limitation for Microsoft (both as processor, and as authorised further processing controller) and the lack of any non conformity findings in the audit commissioned by SLM Rijk[114], these retention periods are not disproportionate.

In sum, the processing of personal data is generally proportional to the purposes. Where such processing is not proportionate in specific use cases, government organisations have the technical means to limit or stop this processing.

14. Rights of data subjects

The GDPR grants data subjects the right to information, access, rectification and erasure, object to profiling, data portability and file a complaint. It is the data controller's obligation to provide information and to duly and timely address these requests. If the data controller has engaged a data processor, the GDPR requires the data processing agreement to include that the data processor will assist the data controller in complying with data subject rights requests.

As discussed in Section 5, Microsoft qualifies as data processor for all data processing in the context of the Azure AD, and has to assist the controller with any data subject access requests. Organisations can block the transfer of personal data to Microsoft from the *on premise* Dynamics server, to prevent all data processing by Microsoft.

[114] SLM Microsoft, Google and AWS Rijk, Memo Audit on Microsoft 2020, URL: https://slmmicrosoftrijk.nl/?sdm_process_download=1&download_id=3063j.

14.1 Right to information

Data subjects have a right to information. This means that data controllers must provide people with easily accessible, comprehensible and concise information in clear language about, inter alia, their identity as data controller, the purposes of the data processing, the intended duration of the storage and the rights of data subjects. As quoted above in Section 13, the EDPB explains in its Guidelines on transparency that controllers should clearly explain the most important consequences of the processing. *"[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data."*[115]

With the help of this DPIA, government organisations that wish to use the *on-premise* Dynamics server in combination with the Azure AD can inform both their external relations and their employees about the scope and purposes of the data processing.

14.2 Right to access

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

As a data processor for the Azure AD Microsoft enables government organisations (as customers) to upload, change and delete the Content Data (account data) in the AD. Organisations can work with federated identity to pseudonymise the Account Data. Microsoft also offers access to the Diagnostic Data about the use of the Azure AD. With these tools, organisations can provide access to employees to all relevant Account Data registered in the directory, and to the Diagnostic Data about their use of the authentication service.

Government organisations have access to the Content and the *on premise* logs of the *on-premise* Dynamics server. With this access, they can fully answer any request by an external data subject whose personal data are stored in, or processed by, the Dynamics CRM.

Microsoft did not provide access to the Telemetry Data from the *on-premise* server, but has explained these data are obsolete, and not used for any purpose.

In sum, if organisations follow the advise in this DPIA to block Telemetry Data on pre-2018 installs of the *on-premise* server, both employees and external data subjects can fully exercise their data access rights.

14.3 Right of rectification and erasure

Thirdly, under Article 16 to 17 GDPR, data subjects have the right to have inaccurate or outdated information corrected, incomplete information completed and - under certain circumstances - personal information deleted.

The government organisation has the ability to delete data from Dynamics CRM when a data subject who is a contact person of the Council so requests. It can also

---

[115] The EDPB has adopted the Article 29 Working Party guidelines WP 260 rev 1, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and Adopted on 11 April 2018, Par. 41.

update data, where necessary. In the tested setup, however, the deleted or outdated data were still available for some time in de audit tables. This enables the government organisation to reverse a mistaken deletion or correction, but at the same time infringes on the right of the data subject to have their data deleted or incorrect data corrected. As was discussed in Section 14.2 of this DPIA, this can only be legitimate if the recovery data is stored for a short time only.

14.4 Right to object to processing, including profiling

Fourthly, under Article 21 GDPR, data subjects have the right to object to an exclusively automated decision if it has legal effects. When processing data about the use of Dynamics CRM there are no known decisions that the Council or Microsoft makes that have legal consequences or other noteworthy consequences for the rights and freedoms of the data subjects. Therefore, this specific right of objection does not apply in this case.

14.5 Right to data portability

This right has no meaning for the processings investigated for this DPIA, as the right to data portability is limited to processings that rely on consent or contract.

Conclusion

Where Content Data are concerned, the government organisation is able to honour the rights of the data subject, but only if the processing of data in audit tables is limited to a very short period, if the data subject has requested deletion or correction. With regard to the (obsolete) Telemetry Data, Microsoft as controller cannot honour these rights as the data are discarded upon receipt. Government organisations must therefore block the processing.

Part C. Discussion and Assessment of the Risks

This part concerns the description and assessment of the risks for data subjects. This part starts with an overall identification of the risks in relation to the rights and freedoms of data subjects, as a result of the processing of metadata and content in the Diagnostic Data. The risks are described for government employees, and for other data subjects that interact with government, in the case of this DPIA contact persons of the Council.

15. Risks

15.1 Identification of risks

The processing of personal data through Dynamics CRM by the Council and the associated Diagnostic Data (including Telemetry Data, cookie data, and audit logs) by Microsoft results in five data protection risks.

1. Possible unlawful continued processing of personal data (including sensitive and special categories of data) in Audit tables.
2. Use of tracking pixels in newsletters without consent.
3. Inability to exercise data subject rights.
4. Lack of legal ground for the collection of legacy server Telemetry Data (Microsoft controller).
5. Transfer of Account Data to Singapore, Australia and the USA.

Below these five risks are assessed against the likelihood of the occurrence of these risks and the severity of the impact.

The UK data protection commission ICO provides the following guidance: *"Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk."*[116] In order to weigh the severity of the impact, and the likelihood of the harm for these generic risks, this report combines a list of specific risks with specific circumstances of the specific investigated data processing.

15.2 Assessment of risks

15.2.1 Possible unlawful further processing of special categories of data in Audit tables

The fact that all changes to the Dynamics database get recorded in the audit tables creates the risk that Dynamics CRM processes special categories of personal data in violation with the prohibition to process these data. The processing of these data is prohibited unless an exception applies.

Depending on the exception that applies to the processing of these data by the government organisation, the exception may not apply to the further processing in the audit tables. In addition, depending on the exception, additional restrictions on access to these data may be circumvented by their inclusion in the audit tables, where set restrictions do not necessarily apply. Because government organisations are able to exclude fields with special categories of data from the audit logs, the

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

chance that these sensitive data are retained too long is low. Even though the impact associated with this risk is high due to the nature of the data, the risk can be assessed as low.

15.2.2 Use of tracking pixels without consent

Microsoft has programmed the marketing module in Dynamics to include a tracking pixel in each mail sent. This allows Dynamics to determine when and how often an email is opened by the recipient and generate (*on premise)* analytics, or online dashboards. Based on the ePrivacy Directive this retrieval of information from a recipient's device requires consent. Because the pixel is included by default, there is a high likelihood that the government organisation does not ask for specific and informed consent from all subscribers for this tracking behaviour. As described in Section 5.3, Microsoft may even be qualified as a joint controller with its customers for this data processing.
However, in reply to this DPIA Microsoft has created an option for customers to disable the tracking pixel. Assuming government organisations will follow this recommendation, the likelihood of unlawful processing is low. Even though the impact is high, as the recording of reading behaviour infringes on the fundamental right to communications secrecy, the data protection risk is low.

15.2.3 Inability to exercise data subject rights

When the tests were initially performed for this DPIA, Microsoft did not respond to a Data Subject Access Request for data about the *on premise* Dynamics server, even though the server (installed before 2018) sent (legacy) Telemetry Data to Microsoft. As a result of this DPIA, Microsoft has provided policies for organisations to block sending these data to Microsoft. Microsoft has also explained the background of other observed data streams. As processor for the Azure AD and Office services, Microsoft would have provided access through its online portals for admins, if the requests were filed in time.

With regard to the tracking pixel, the possibility for individual recipients to opt-out does not stop the collection of personal data with the pixel, but will lead to anonymisation of the personal data. Such an option to opt-out cannot comply with the legal requirement of consent. That is, the right of a data subject to freely decide to provide, or not to provide consent, and to stop all future processing after withdrawing consent.

Assuming government organisations will follow the advise to disable the tracking pixel and block the legacy telemetry data, the risk of an inability to exercise data subjects rights will not materialise, and can therefore be assessed as low.

15.2.4 Lack of legal ground for the collection of legacy server Telemetry Data (Microsoft controller)

As described in Section 5.4, Microsoft acts as data controller for the legacy Telemetry Data it collects from the *on premise* Dynamics server. This means Microsoft reserves the right to process these data for all of the 19 purposes mentioned in its general (consumer) privacy policy, including marketing and profiling. Microsoft itself acknowledges that the collection of these Software Quality Metrics data ("SQM") is not necessary, as the *on premise* Dynamics server is designed to offer air gapped deployment. Microsoft has provided the policy rules to block this data stream.
Even though the impact of the processing of these data for Microsoft's own commercial purposes could be high in specific circumstances, the likelihood that these risks materialise is zero if organisations follow the recommendation to apply the policy rules.

15.2.5 Transfer of Azure Account Data to Singapore, Australia and the USA.

The transfer of personal data outside of the European Economic Area (EEA) poses a risk in itself, because the standard of protection of personal data in most countries in the world is lower than in the European Union.[117] This section describes two related transfer risks: transfer to Microsoft in the USA, and transfer to a subprocessor in third countries.

Though Microsoft is already processing most personal data from its EU customers within the EU Data Boundary, the Azure AD is excluded. As described in Section 7.1 the Azure AD was designed as a non-regional service, even though most customer data from EU customers are already stored and processed in the EU Data Boundary. Microsoft mentions three reasons to continue to process the Azure AD data in the USA: (i) phone calls for multifactor authentication, (ii) when an end user visits the USA and (iii) use of 3d party messaging services from Apple or Google.[118] Organisations can largely prevent the occurrence of these exceptions, or use an *on premise* AD. In view of the new adequacy decision for the USA, the impact of this risk must also be assessed as low.

Additionally, in its list of subprocessors for its online services, Microsoft mentions the use of Arkose Labs Inc, a subprocessor for the Azure AD with offices in Ireland, Singapore, Australia and the USA. However, as explained in Section 7.2, Microsoft has explained that it uses the company to show Captchas to its consumer customers, but never to Enterprise customers. As Microsoft does not mention any other subprocessors for the Azure AD, the likelihood of transfer of the account data to third countries is low. Therefore, the risk can also be assessed as low.

Summary of risks

This DPIA describes five separate risks. In reply to this DPIA, Microsoft has offered technical measures or information with which customers can mitigate most of the risks.

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

[118] Microsoft, Data residency and customer data for Azure Multi-Factor Authentication, 30 January 2023, URL: https://learn.microsoft.com/en-gb/azure/active-directory/authentication/concept-mfa-data-residency

Part D. Description of risk mitigating measures

Part D describes the proposed (counter-)measures. Part C of this DPIA has identified five data protection risks. The risks are assessed as low, if government organisations take the recommended risk mitigating measures.

16.1 Risk mitigating measures

The following section contains a table of the mitigating technical and organisational, measures that government organisations can and should take to reduce high risks.

Table 2: Measures to be taken by the government organisation and Microsoft to mitigate high risks

Risk no.	Risk	Measures government organisation	Measures Microsoft
1.	Possible unlawful continued processing of personal data (including sensitive and special categories of data) in Audit tables.	Review the lawfulness of including sensitive and special categories of data in the Audit tables, or follow the guidance from Microsoft to exclude these data from the Audit tables.	- no measures necessary, guidance is available at https://learn.microsoft.com/en-us/dynamics365/customerengagement/*on-premise*s/admin/audit-data-user-activity?view=op-9-1#enable-or-disable-entities-and-fields-for-auditing.
2.	Use of tracking pixels in newsletters without consent.	Update the software to benefit from the new option, and disable use of tracking pixels in newsletters sent with the marketing module.	- no measures necessary, Microsoft enables admins to disable the tracking pixel via https://learn.microsoft.com/en-us/dynamics365/marketing/privacy-use-features .
3.	Inability to exercise data subject rights.	It is possible to use Dynamics as *on-premise* software and not use cloud services such as the Azure AD.	- no measures necessary, admins have access to all Content Data and logs.

		If a government organisation uses the Dynamics cloud services, they can obtain access to Content Data via the Security & Compliance center, and the Azure export tool for system-generated logs.	Information about export of Content and Diagnostic Data in the cloud services is available at https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-data-subject-requests#data-subject-request-admin-tools.
4.	Lack of legal ground for collection of legacy server Telemetry Data (Microsoft controller).	Block sending of legacy server Telemetry Data (possibly with the help of an implementation partner).	- no extra measures necessary, Microsoft no longer collects these data in newer server versions.
5.	Transfer of Account Data to Singapore, Australia and the USA	Prevent the 3 situations in which the Azure AD data are transferred to the USA.	Complete the EU Data Boundary for the Azure AD, regardless of the new adequacy decision.
		Use pseudonyms if the identity of specific employees should remain secret. If that is insufficient, do not use the Azure AD cloud for authentication, only the *on premise* AD.	No measures necessary with regard to Arkose Labs Inc, as this subprocessor is not used for Enterprise customers

Conclusion
Microsoft has taken adequate technical measures or provided relevant information to mitigate the initially identified 5 high risks. If the government organisations apply the recommended risk mitigating measures in this DPIA, there are no known high or low data protection risks.

Microsoft can take one more measure to solve the low risk of transfer of personal data to the USA, if organisations use the Azure AD cloud service for authentication, to exclusively process the Azure AD data in the EU Boundary.

Annex 1

Policy rules to block legacy Telemetry Data - provided by Microsoft

1. With all the recent versions of the D365 On Premises platform, the user interface that allowed configuration of software quality metrics (SQM) is removed. Consequently, the only way to interact with the setting is via PowerShell.

2. To see SQM settings via PowerShell, first you need to use a Windows PowerShell Cmd prompt on the Deployment Server (the server hosting the deployment).

Important note: you must use the Windows PowerShell cmd prompt. You cannot use the PowerShell 7 cmd prompt.

These instructions explain how to setup PowerShell the module to work: Overview of Dynamics 365 Customer Engagement PowerShell module | Microsoft Learn

3. To work with SQM data you will use the **Get** and **Set-CrmSetting** commands:

You first must look up the "SqmSettings" type. (Documented here: Update deployment configuration settings | Microsoft Learn)

Add-PSSnapin Microsoft.Crm.Powershell
This will load the module into the local PowerShell session

Get-CrmSetting -SettingType SqmSettings
Returns the current settings for the SqmSettings

For example:
SqmEnabled ExtensionData
---------- -------------
False System.Runtime.Serialization.ExtensionDataObject
Indicates that the Sqm Feature is disabled.

4. If it is determined SQM is enabled, use Set-CrmSetting to deactivate:

$currentSqmSetting = Get-CrmSetting -SettingType SqmSettings
$currentSqmSetting.SqmEnabled = $false
Set-CrmSetting -Setting $currentSqmSetting