Ernst & Young Accountants LLP
Cross Towers, Antonio Vivaldistraat 150
1083 HP Amsterdam, Netherlands
Postbus 7883
1008 AB Amsterdam, Netherlands

Tel: +31 88 407 10 00
Fax: +31 88 407 10 05
ey.com

CONFIDENTIAL
Dutch Ministry of Justice and Security
Attn. Mr. H.M. Barnard
Postbus 10451
2501 HL DEN HAAG

Amsterdam, 13 March 2024 REQ6840983/AC/lg

Assurance report related to personal data protection as part of Legitimate Business Operations

Dear Mr. Barnard,

Ernst & Young Accountants LLP (hereafter: EY or we) has been engaged by the Dutch Ministry of Justice and Security to conduct an examination of Microsoft's data protection as part of Legitimate Business Operations related to use of Microsoft Teams with inclusion of Microsoft Azure AD in the context of Microsoft Teams. By means of this assurance report we inform you about our findings.

In appendix 1 we included the control objectives and related controls in scope of our examination, as well as the nature, timing and results of our test of these controls with regard to Microsoft's internal controls concerning Microsoft's data protection as part of Legitimate Business Operations.

Finally, we would like to remind you of the restrictions on use and distribution, as stated in the assurance report. We trust that this information has been sufficient, and we are ready and willing to answer any further questions.

Yours sincerely,
Ernst & Young Accountants LLP

signed by P. (Peter) Kornelisse RE
Partner

Ernst & Young Accountants LLP
Cross Towers, Antonio Vivaldistraat 150
1083 HP Amsterdam, Netherlands
Postbus 7883
1008 AB Amsterdam, Netherlands

Tel: +31 88 407 10 00
Fax: +31 88 407 10 05
ey.com

Assurance report of the independent IT auditor

To: Dutch Ministry of Justice and Security

Our qualified opinion

On request of the Dutch Ministry of Justice and Security and the scope as agreed mutually beforehand with Microsoft, we have examined Microsoft's description of controls as included in appendix 1 to the assurance report relating to Legitimate Business Operations concerning Aggregated reporting – (A) Compensation, (B) Customer billing and account management, (C) Financial reporting –, and (D) Legal obligations, for Microsoft Teams with inclusion of Microsoft Azure AD in the context of Microsoft Teams, throughout the period from 1 January 2023 to 31 March 2023 (the description of controls in appendix 1). We also examined the design and operating effectiveness of controls related to the control objectives stated in the description of controls in appendix 1 (control objectives).

In our opinion, except for the matters described in the "Basis for our Qualified Opinion" section, in all material respects for Legitimate Business Operations concerning Aggregated reporting – (A) Compensation, (B) Customer billing and account management, (C) Financial reporting –, and (D) Legal obligations:

- The description of controls in appendix 1 fairly presents the controls that were designed and implemented throughout the period from 1 January 2023 to 31 March 2023
- The controls related to the control objectives were suitably designed to achieve the control objectives if the controls operated effectively throughout the period from 1 January 2023 to 31 March 2023
- The controls tested operated effectively to achieve the control objectives throughout the period from 1 January 2023 to 31 March 2023

The criteria applied in forming our opinion are the criteria described in the "Applicable criteria" section.

Our opinion has been formed on the basis of the matters outlined in this assurance report. The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying appendix 1 (our description of tests and results).

Basis for our qualified opinion

The basis of our qualified opinion pertains on only to the Legal obligations Legitimate Business Operations, and is formed by the controls referenced in this section below. Due to the nature of the services of Microsoft for some controls the operating effectiveness could not be determined, as these could not be evidenced by Microsoft due to sensitivity of the policies and procedures, related to legal orders and legally binding requests only.

Consequently, we were unable to determine that the following control objectives were achieved throughout the audit period from 1 January 2023 to 31 March 2023:

- CO-BO-12.2: Controls must provide reasonable assurance that systems in use by LENS (part of legal team) to manage and fulfill requests, are subject to Identity and Access (IDA) mechanisms. These IDA mechanisms enable segregation of duties and management oversight, and prevent disclosing data without formal approval.
  - We determined that the control is designed and implemented by Microsoft, but we were unable to determine that controls CBO12.3, CBO12.4, CBO12.5 were operating effectively throughout the audit period.

We refer to our description of tests and results in appendix 1 for further details.

We performed our examination in accordance with Dutch law and Dutch Guideline 3000A "Assurance-opdrachten door IT-auditors (attest-opdrachten) (assurance engagements performed by IT auditors (attestation engagements)) as issued by the professional association for IT auditors in the Netherlands (NOREA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), 'Assurance Engagements Other than Audits or Reviews of Historical Financial Information", issued by the International Auditing and Assurance Standards Board]. This engagement is aimed to obtain reasonable assurance. Our responsibilities in this regard are further described in the "IT auditor's responsibilities" section of our assurance report.

We have complied with the NOREA "Reglement Gedragscode" (Code of Ethics for IT Auditors, a regulation with respect to integrity, objectivity, professional competence and due care, confidentiality and professional behavior) and with the "Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten" (ViO, Code of Ethics for Professional Accountants, a regulation with respect to independence). The Code of Ethics for IT Auditors and the NOREA Guidelines related to assurance engagements are at least as demanding as the International Code of Ethics for Professional Accountants (including International Independence Standards) of the International Ethics Standards Board for Accountants (the IESBA Code).

For the execution of this assurance engagement, use is made of the option included in Article 3 paragraph 7 of the ViO whereby the users (Dutch Ministry of Justice and Security, also on behalf of other government entities) agree to the fact that EY is independent of the subject matter of the assurance engagement and the responsible persons, but is not independent of the responsible entity (Microsoft Corporation) as a result of the existing alliance between EY and Microsoft, as confirmed in our engagement letter with the Dutch Ministry of Justice and Security, also on behalf of other users of this report.

We believe that the assurance evidence we have obtained is sufficient and appropriate to provide a basis for our qualified opinion.

Applicable criteria

For this engagement, the following criteria apply:

- The description of controls in appendix 1 provides a complete and accurate overview of the controls that have been designed and implemented to achieve the control objectives.
- The description of controls in appendix 1 does not omit or distort information relevant to the control objectives or the controls related to the control objectives. If applicable, the description of controls in appendix 1 states the controls performed by another organization (inclusive method) or the controls of Microsoft to monitor the effectiveness of controls at other organizations (carve-out method).
- The description of controls in appendix 1 includes relevant details of changes to controls throughout the period from 1 January 2023 to 31 March 2023.
- The risks that threatened the achievement of the control objectives, have been identified.
- The controls identified in the description of controls in appendix 1 would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives from being achieved.
- Controls were consistently applied as designed, including manual controls applied by individuals who have the appropriate competence and authority throughout the period from 1 January 2023 to 31 March 2023.

Matters related to the scope of our examination

Non-occurrence of circumstances that warrant the operation of controls

As noted in our description of tests and results in appendix 1, circumstances that warrant the operation of the controls: CBO11.1, CBO11.2, CBO11.3, CBO11.4, CBO12.1, CBO12.2, CBO13.1, CBO13.2, CBO13.3, CBO13.4, 13.5, 13.6, 13.7 did not occur. As a result, we did only examine test of design and implementation, and did not examine the operating effectiveness of these controls during the period from 1 January 2023 to 31 March 2023.

No examination of other information

The information included in appendix 2 is presented by management of Microsoft to provide additional information and is not a part of the description of controls in appendix 1. Accordingly, we express no opinion on this information.

Our opinion is not modified in respect of these matters.

Limitations of a description and to controls at an organization

The control objectives are specified by Microsoft and may not, therefore, include every aspect of Microsoft's internal controls related to personal data protection as part of Legitimate Business Operations that each individual user may consider important. Because of their nature, controls at an organization may not prevent, or detect and correct, all errors or omissions. Also, the projection to the future of conclusions about the suitability of the design or operating effectiveness of the controls to achieve the control objectives is subject to the risk that controls at an organization may become ineffective.

Restrictions on use and distribution

Our assurance report and the description of tests of controls and results thereof in our description of tests and results, are intended solely for the information and use of Microsoft, the Dutch Ministry of Justice and Security, all entities under the MBSA contracted by the Dutch Ministry of Justice and Security, and their auditors, who have a sufficient understanding to consider our assurance report and our description of tests and results, along with other information, including information about controls operated by Microsoft, when assessing the risks of material errors or omissions relating to personal data protection as part of Legitimate Business Operations. Our assurance report and our description of tests and results should only be used for the intended purpose by the intended users and should not be distributed to or used by other parties. Without our prior written consent, it is not allowed to publish or distribute our assurance report and our description of tests and results to others, in whole or in part, or to quote from or refer to our assurance report or our description of tests and results whether or not with acknowledgement.

Responsibilities of Microsoft

Microsoft is responsible for:

- Preparing the description of controls in appendix 1 and fairly presenting the controls as designed and implemented relating to the personal data protection as part of Legitimate Business Operations in accordance with the applicable criteria
- Specifying the control objectives and stating them in the description of controls in appendix 1
- Identifying the risks that threaten the achievement of the control objectives
- Designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the control objectives

Furthermore, Microsoft is responsible for such internal control as it determines is necessary to enable the preparation of the description of controls in appendix 1 that is free from material misstatement, whether due to fraud or error, and for monitoring of controls to assess their effectiveness, to identify deficiencies and to take corrective actions.

IT auditor's responsibilities

Our responsibility is to plan and perform our examination in a manner that allows us to obtain sufficient and appropriate assurance evidence for our opinion.

Our examination has been performed with a high, but not absolute, level of assurance, which means we may not detect all material errors and fraud during our examination.

We apply the "Reglement Kwaliteitsbeheersing NOREA" (RKBN, a standard on quality control) that is at least as demanding as the International Standard on Quality Management (ISQM1), and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional guidelines and applicable legal and regulatory requirements.

Our examination included among others:

- Identifying and assessing the risks that the description of controls in appendix 1 does not fairly present the controls and that the controls were not suitably designed or working effectively to achieve the control objectives throughout the period from 1 January 2023 to 31 March 2023, whether due to errors or fraud, and designing assurance procedures responsive to those risks in order to obtain assurance evidence that is sufficient and appropriate to provide a basis for our opinion
- Evaluating the overall presentation of the description of controls in appendix 1 and the suitability of the control objectives
- Performing procedures to obtain assurance evidence about the fair presentation of controls in the description of controls in appendix 1 and the suitability of the design of the controls to achieve the control objectives
- Testing the operating effectiveness of those controls necessary to provide reasonable assurance that the control objectives were achieved.

Amsterdam, 13 March 2024

Ernst & Young Accountants LLP

signed by P. (Peter) Kornelisse
Partner

Appendix 1: Examination of controls

1.1 Control environment and processes, control objectives and controls

The internal control environment encompasses the collective impact of various factors on achieving or improving the effectiveness of the controls defined by Microsoft. In determining the nature, timing, and extent of our work to evaluate the controls defined by Microsoft, we have considered the following aspects of the internal control environments of Microsoft: organizational structure, policies and procedures, processes for risk management, and processes for management monitoring.

The control objectives on the following pages are defined by and the responsibility of Microsoft. Microsoft is responsible for listing the control objectives and specifying the related controls. The controls related to these control objectives have been sourced from the control framework of Microsoft that has been established for the purpose of this audit. As these controls are part of the internal used control framework, the numbering of Microsoft is used (objective 1-6 and 11-13). The executing of the test procedures and the reporting of the observations are the responsibility of EY. The following control objectives are in scope:

- CO-BO-1.1: Controls must provide reasonable assurance to ensure only authorized and appropriate access to all categories of personal data.
- CO-BO-2.1: Controls must provide reasonable assurance that essential mechanisms for the appropriate pseudonymization of personal data are defined and observed within Microsoft.
- CO-BO-3.1: Controls must provide reasonable assurance that essential mechanisms for appropriate aggregation and pseudonymization of personal data are defined and observed within Microsoft.
- CO-BO-4.1: Controls must provide reasonable assurance to ensure reports used for Business Operations are generated and maintained such that only required information is disclosed subject to appropriate approvals.
- CO-BO-5.1: Controls must provide reasonable assurance in preventing unauthorized access to the reporting portals managed by IDEAS.
- CO-BO-6.1: Controls must provide reasonable assurance in preventing unauthorized access to datasets managed by IDEAS.
- CO-BO-11.1: Controls must provide reasonable assurance that Microsoft follows strict processes and procedures to evaluate, assess and handle third party legal demands for customer data. These processes and procedures must align to the contractual commitments with Customers concerning protection and disclosure of Customer Data and Personal Data.
- CO-BO-11.2: Controls must provide reasonable assurance that the Microsoft LENS team is sufficiently qualified and ensures appropriate skills and competences to handle complex legal orders or requests.

- CO-BO-12.1: Controls must provide reasonable assurance that the LENS team follows and maintains processes and systems to manage requests for enterprise data, which prevent disclosing data without Attorney approval and enable data residency during case handling.
- CO-BO-12.2: Controls must provide reasonable assurance that systems in use by LENS to manage and fulfill requests, are subject to Identity and Access (IDA) mechanisms. These IDA mechanisms enable segregation of duties and management oversight, and prevent disclosing data without formal approval.
- CO-BO-13.1: Controls must provide reasonable assurance that the Microsoft LENS team supports transparency reporting and prevent over disclosure, by tracking, monitoring and logging all activities during case handling and data disclosure.
- CO-BO-13.2: Controls must provide reasonable assurance to prevent over disclosure and make sure data is minimized to what is compelled and responsive to the request.

The controls relating to the control objectives above as included in this assurance report are further detailed by Microsoft into control activities (not included in our assurance report), and these are the basis for our testing procedures.

The scope includes Microsoft's Legitimate Business Operations concerning Aggregated reporting – (A) Compensation, (B) Customer billing and account management, (C) Financial reporting –, and (D) Legal obligations, for the IT component Microsoft Teams with inclusion of Microsoft Azure AD in the context of Microsoft Teams. The Legitimate Business Operations concerning Aggregated reporting – (A) Compensation, (B) Customer billing and account management, (C) Financial reporting – is the scope of control objectives CO-BO-1.1 to CO-BO-6.1. The Legitimate Business Operations concerning (D) Legal Obligations is the scope the control objectives CO-BO-11.1 to CO-BO-13.2.

Both the scope and the control framework have been confirmed by the Dutch Ministry of Justice and Security, Microsoft, and EY prior to the execution of the test procedures.

1.2 Control testing

In the table below, we have outlined our test procedures and we have described the performed testing activities.

Test procedure	Description testing activities
Inquiry (interview)	Inquiring of appropriate Microsoft personnel that, in our judgment, may have relevant information.
Inspection (examination)	Read documents, reports and electronic records that contain an indication of performance of the control. This includes, among other things, reading of (management) reports to assess whether the specified control is properly monitored, controlled and resolved on a timely basis.
Observation	View the application of specific controls by Microsoft personnel.
Re-performance	Re-perform the operation of a control to ascertain that it was performed correctly.

1.1.1 Testing of Information Produced by the Entity

For tests of controls requiring the use of information produced by the entity (e.g., controls requiring system-generated populations for sample-based testing), we perform a combination of the following procedures where possible based on the nature of the information produced by the entity to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspected the source of the information produced by the entity, (2) inspected the query, script, or parameters used to generate the information produced by the entity, (3) tied data between the information produced by the entity and the source, and/or (4) inspected the information produced by the entity for anomalous gaps in sequence or timing to determine the data is complete and accurate. Furthermore, in addition to the above procedures, for tests of controls requiring management's use of information produced by the entity in the execution of the controls (e.g., periodic reviews of user access listings), we inspected management's procedures to assess the validity of the source and the completeness, accuracy, and integrity of the data or reports.

1.3 Control objectives and related controls, audit procedures and observations

Below, for Microsoft's defined control objectives and controls, and the results of our performed procedures.

CO-BO-1.1			
Controls must provide reasonable assurance to ensure only authorized and appropriate access to all categories of personal data.			
Reference	**Control description**	**Test procedures**	**Observations**
CBO1.1	Microsoft has centralized privacy policies, standards, and data handling documentation that are reviewed at least annually.	Inquired M365 Privacy Program Owner and M365 Privacy Architect to understand the review process of policies, standards, and data handling documentation. Obtained and inspected evidence of Microsoft privacy standards, data taxonomy and data handling standards to determine if this documentation is reviewed at least annually.	Exception noted. Per inquiry of the M365 Privacy Program Owner and the M365 Privacy Architect and inspection of documentation an annual review of the Microsoft privacy standards and data taxonomy is in place. Per inquiry of the M365 Privacy Program Owner and the M365 Privacy Architect we were informed that there is no process in place for annual review and approval of the Data Handling Standards by the Microsoft Customer Data Governance Board. Per inquiry of the M365 Privacy Program Owner and the M365 Privacy Architect and per inspection of e-mail conversations and meeting minutes we determined that the content of the Data Handling Standards is frequently discussed during the weekly meetings of the Privacy teams, limiting the risk of these document becoming outdated. Moreover, per inquiry of the M365 Privacy Program Owner and the M365 Privacy Architect

CO-BO-1.1			
Controls must provide reasonable assurance to ensure only authorized and appropriate access to all categories of personal data.			
Reference	**Control description**	**Test procedures**	**Observations**
			we were informed that the Data Handling Standards are used daily by a large number of Microsoft employees and are rarely subject to change. No further exceptions noted.
CBO1.2	Prior to accessing pseudonymized data, engineers are required to complete privacy training.	Inquired M365 Privacy Program Owner and M365 Data Privacy Governance Engineer – Product Manager to understand the access management process related to training requirements. Obtained and inspected evidence related to the privacy training. Reperformed the control to ascertain that users can only request access when all the user fulfills all the requirements, including training.	No exceptions noted.

CO-BO-1.1

Controls must provide reasonable assurance to ensure only authorized and appropriate access to all categories of personal data.

Reference	Control description	Test procedures	Observations
		For all users with access to the relevant environment in the last 90 days, we determined that the user fulfills the training requirements. For all users that did not fulfill the training requirements, we determined the user did not have access.	
CBO1.3	Microsoft personnel that have access to pseudonymized data, are trained on all applicable policies and obligations related to the use of that data.	Inquired M365 Privacy Program Owner and M365 Data Privacy Governance Engineer – Product Manager to understand the requirements related to training and attestation to gain access to pseudonymized data. Obtained and inspected the settings in the source code to determine that an attestation is only valid for 90 days. Reperformed the control to ascertain that users can only request access when all the user fulfills all the requirements, including attestation.	No exceptions noted.

CO-BO-1.1

Controls must provide reasonable assurance to ensure only authorized and appropriate access to all categories of personal data.

Reference	Control description	Test procedures	Observations
		Reperformed the control to ascertain that the attestation is only valid for 90 days from the date the user signs the attestation. For all users with access to the relevant environment in the last 90 days, we determined that the user fulfills the attestation requirements. For all users that did not fulfill the attestation requirements, we determined the user did not have access.	
CBO1.4	Access to telemetry data stores with pseudonymized data are governed by processes to ensure appropriate access, training and approvals by a manager.	Inquired M365 Privacy Program Owner and M365 Data Privacy Governance Engineer – Product Manager to understand the requirements and process for gaining access to telemetry data stores. Reperformed the control to ascertain that manager approval is required in order for a user to gain access to	No exceptions noted.

CO-BO-1.1

Controls must provide reasonable assurance to ensure only authorized and appropriate access to all categories of personal data.

Reference	Control description	Test procedures	Observations
		telemetry data stores, and that the user cannot gain access in case the manager denies the request for access.	
CBO1.5	Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning user, group or non-human account access in scope production assets to prevent unauthorized access to pseudonymized personal data.	Inquired IDEAs Senior Product Manager and IDEAs Principal Program Manager to understand the process for gaining access to the internal platform where reports (which may contain pseudonymized personal data) are accessible. Reperformed the control to ascertain that manager approval is required for a user to gain access to the platform for accessing reports, and that the user cannot gain access in case the manager denies the request for access. For the access requests in the audit period, we determined that an Approver is linked to every request that approved or denied the request.	No exceptions noted.

CO-BO-1.1

Controls must provide reasonable assurance to ensure only authorized and appropriate access to all categories of personal data.

Reference	Control description	Test procedures	Observations
CBO1.6	Prevent unauthorized access or change to EUII, EUPI and content while in transit between Microsoft operated systems.	Inquired Program Manager GRC Global to understand the measures taken to prevent unauthorized access or change while data is in transit. Obtained and inspected service configurations related to encryption of internal and external network transfers. Obtained and inspected service logs for all established connections during the audit period to determine that encryption with TLS1.2 was active.	No exceptions noted.

CO-BO-2.1

Controls must provide reasonable assurance that essential mechanisms for the appropriate pseudonymization of personal data are defined and observed within Microsoft.

Reference	Control description	Test procedures	Observations
CBO2.1	Use data classification guidelines and data handling policies to instruct	Inquired M365 Privacy Program Owner and Program Manager GRC Global to understand which guidelines and	No exceptions noted.

CO-BO-2.1

Controls must provide reasonable assurance that essential mechanisms for the appropriate pseudonymization of personal data are defined and observed within Microsoft.

Reference	Control description	Test procedures	Observations
	personnel to handle data used for business operations appropriately.	policies are present to instruct personnel on data handling for business operations, and how personnel is trained on these topics. Obtained and inspected screenshots of the training and determined that personnel is trained on using the guidelines and standards. Obtained and inspected screenshots of internal (privacy) assessments and determined the guidelines are used when performing reviews to validate the allowable processing of data.	
CBO2.2	Microsoft periodically evaluates data processing for products or features through a privacy review. These privacy reviews assess System Generated Logs data flows.	Inquired M365 Privacy Program Owner and Program Manager GRC Global to understand the evaluation of data processing, both periodically for existing products as well as when releasing new products or features.	Exception noted. For one (1) of the seven (7) selected features released during our audit period we determined that one required task in the privacy review, Data Profile, was closed without being executed, due to a human error. Per inquiry of the Privacy Program Owner for Office 365 and Intelligent Services and per inspection of the

CO-BO-2.1

Controls must provide reasonable assurance that essential mechanisms for the appropriate pseudonymization of personal data are defined and observed within Microsoft.

Reference	Control description	Test procedures	Observations
		Obtained and inspected screenshots of the settings enforcing privacy reviews. Observed during the meeting that these settings are in place. Obtained and inspected screenshots of the DPIA for O365 Enterprise Services – Teams to determine the DPIA has been updated and reviewed by the Data Protection Officer. Reperformed the control to ascertain that a privacy review task is triggered based on the data properties related to the product or feature, and that this review is performed and signed off by a Privacy Manager. Determined that system generated logs are included as part of the review task. For a sample of features released during the audit period, we determined	Privacy Review and associated evidence we determined that a privacy review was performed for this feature. No further exceptions noted.

CO-BO-2.1

Controls must provide reasonable assurance that essential mechanisms for the appropriate pseudonymization of personal data are defined and observed within Microsoft.

Reference	Control description	Test procedures	Observations
		whether a privacy review was required and performed.	
CBO2.3	Microsoft reduces risk of handling personal data by creating pseudonymous identifiers within the Customer's Azure Active Directory and use that in dependent systems.	Inquired IDEAs Senior Program Manager and Privacy Champion to understand the process of creating pseudonymous identifiers within the Customer's Azure Active Directory. Reperformed the control to ascertain that once a user has been created, a (pseudonymous) identifier is automatically assigned to this user. We further determined that this user ID is associated with user information and is used by dependent systems to retrieve information about the user.	No exceptions noted.
CBO2.4	Microsoft cannot modify pseudonymized identifier (EUPI) once it has been generated which prevents alteration.	Inquired IDEAs Senior Program Manager and Privacy Champion to understand the immutability of the	No exceptions noted.

CO-BO-2.1

Controls must provide reasonable assurance that essential mechanisms for the appropriate pseudonymization of personal data are defined and observed within Microsoft.

Reference	Control description	Test procedures	Observations
		pseudonymized identifier once it has been generated. Obtained, inspected and observed the source code settings to determine the generated user ID is immutable. Reperformed the control to ascertain that the pseudonymized user ID is immutable once generated.	
CBO2.5	Microsoft pseudonymizes personal data from EUII (End User Identifiable Information) to EUPI (End User Pseudonymous Identifiers) to reduce personal data processing risk and to meet Microsoft's policies in accordance with DPA.	Inquired M365 Privacy Program Owner, Principal Engineering Manager and Senior Program Manager – Privacy to understand the process of pseudonymization of personal data (EUII to EUPI). Obtained and inspected code to determine events are logged, scanned and tagged as personally identifiable information (PII) personally identifiable information (PII) when applicable.	No exceptions noted.

CO-BO-2.1

Controls must provide reasonable assurance that essential mechanisms for the appropriate pseudonymization of personal data are defined and observed within Microsoft.

Reference	Control description	Test procedures	Observations
		Obtained and inspected code commits to determine the measures were implemented during the audit period. Reperformed the control to ascertain that system scans data for personally identifiable information (PII) and tags this as applicable, after which the data is hashed for pseudonymization.	
CBO2.6	Microsoft monitors EUPI storage systems for EUII/CC information that is inappropriately stored in telemetry data stores.	Inquired M365 Privacy Program Owner, Principal Engineering Manager and Senior Program Manager – Privacy to understand the process of scanning for inappropriately stored data in telemetry data stores. Observed configurations in the storage system and determined that measures are taken to scan for end user identifiable information (EUII) and	No exceptions noted.

CO-BO-2.1

Controls must provide reasonable assurance that essential mechanisms for the appropriate pseudonymization of personal data are defined and observed within Microsoft.

Reference	Control description	Test procedures	Observations
		customer content (CC) and determined that the measures apply to the workflow for importing Teams telemetry data. Observed, obtained and inspected evidence to determine that a workflow is in place to trigger creation of an incident ticket and a bugfix in case a leak is found. Inspected change logs to determine this workflow was in place during the audit period. For one sample determined that an incident ticket was created and followed up timely, closing the leak.	

CO-BO-3.1

Controls must provide reasonable assurance that essential mechanisms for appropriate aggregation and pseudonymization of personal data are defined and observed within Microsoft.

Reference	Control description	Test procedures	Observations
CBO3.1	Processing operations on Customer Data and Personal data for Online Services are documented in DPIAs to enable and demonstrate Microsoft's accountability to contractual commitments in the DPA.	Inquired Senior Product Manager and Program Manager GRC Global to understand the process of documenting information on data processing in a DPIA and the DPIA update process. Observed, obtained and inspected relevant parts of the DPIA for (LBO) processing to determine that processing operations are documented in the DPIA, as well as (amongst others) measures contributing to the rights of data subjects and other privacy considerations.	No exceptions noted.
CBO3.2	Microsoft performs aggregation on pseudonymized data to discard user level personal information.	Inquired IDEAs Senior Product Manager and IDEAs Principal Program Manager to understand the process of aggregation on pseudonymized data to discard user level personal information.	No exceptions noted.

CO-BO-3.1

Controls must provide reasonable assurance that essential mechanisms for appropriate aggregation and pseudonymization of personal data are defined and observed within Microsoft.

Reference	Control description	Test procedures	Observations
		Observed, obtained and inspected the code for report building to determine pseudonymized data is aggregated into counts. Reperformed the control to determine that the resulting report does not show pseudonymized data, only aggregated data.	

CO-BO-4.1

Controls must provide reasonable assurance to ensure reports used for Business Operations are generated and maintained such that only required information is disclosed subject to appropriate approvals.

Reference	Control description	Test procedures	Observations
CBO4.1	Data published in IDEAs reports must undergo a privacy review to ensure that the use of personal data is appropriate, and that data being	Inquired Senior Product Manager and Program Manager GRC Global to understand the process of privacy reports for data published in IDEAs reports.	Exceptions noted. For six (6) of the six (6) selected IDEAs reports in which data was published during the audit, we were not able to determine that a Privacy Review was completed prior to processing and

CO-BO-4.1

Controls must provide reasonable assurance to ensure reports used for Business Operations are generated and maintained such that only required information is disclosed subject to appropriate approvals.

Reference	Control description	Test procedures	Observations
	published is at an appropriate level of aggregation.	Obtained and inspected a ticket created for a privacy review for Teams data, and determined the input for the review covers at least the scope of data used, the intended use and the aggregation level. Also determined that the review was performed by a Privacy Manager, who confirmed the data use is allowed in line with policies. For a sample of six IDEAs reports, determined that a privacy review was initiated and approved.	publishing the data in the IDEAs report since there is no technical gate that will prevent an approved user within IDEAs from processing and publishing data without a Privacy Review. For six (6) of the six (6) selected IDEAs reports we determined that a Privacy Review was completed. Per inquiry of the Senior Privacy Product Manager, we were informed that Microsoft has implemented multiple layers of defense including access control, embedded Privacy Champs, and multiparty reviews to mitigate the risk that data may be processed and published in IDEAs reports without the completion of a Privacy Review. No further exceptions noted.
CBO4.2	Microsoft reviews and approves all changes to code in production prior to implementation to prevent unauthorized creation or changes of reports.	Inquired IDEAs Senior Product Manager and Program Manager GRC Global to understand the process of review and approval for changes to code in production prior to implementation.	No exceptions noted.

CO-BO-4.1

Controls must provide reasonable assurance to ensure reports used for Business Operations are generated and maintained such that only required information is disclosed subject to appropriate approvals.

Reference	Control description	Test procedures	Observations
		For a sample of five pull requests, determined that changes to source code (pull requests) are reviewed as part of the deployment process, separation of duties is maintained in code reviews, and reviewer sign-offs are documented prior to deployment to production.	

CO-BO-5.1

Controls must provide reasonable assurance in preventing unauthorized access to the reporting portals managed by IDEAS.

Reference	Control description	Test procedures	Observations
CBO5.1	Requests for access to IDEAs reports are submitted and approved prior to provisioning access.	Inquired IDEAs Senior Product Manager and IDEAs Principal Program Manager to understand the process of access requests and approvals for IDEAs reports.	No exceptions noted.

CO-BO-5.1			
Controls must provide reasonable assurance in preventing unauthorized access to the reporting portals managed by IDEAS.			
Reference	**Control description**	**Test procedures**	**Observations**
		Obtained and inspected evidence outlining different types of reports and requirements for access to these types of reports. Obtained and inspected evidence of an access request and the manager approval of the attestation for this request. For all requests in scope during the audit period, determined that approvers are linked and for all granted access, determined that at least one of the approvers has approved the attestation for the access request.	
CBO5.2	Microsoft requires Microsoft employees to sign an attestation before accessing systems providing access to LBO information.	Inquired IDEAs Senior Product Manager and IDEAs Principal Program Manager to understand the attestation process before accessing systems providing access to LBO information.	No exceptions noted.

CO-BO-5.1

Controls must provide reasonable assurance in preventing unauthorized access to the reporting portals managed by IDEAS.

Reference	Control description	Test procedures	Observations
		Obtained and inspected evidence outlining the Security and Access Policy for the report, which includes submitting an attestation and approval by manager. Reperformed the control to ascertain that a user needs to fill an attestation in order to request access, and the managers needs to approve the attestation.	

CO-BO-6.1

Controls must provide reasonable assurance in preventing unauthorized access to datasets managed by IDEAS.

Reference	Control description	Test procedures	Observations
CBO6.1	Prior to accessing datasets managed by IDEAs, engineers are required to complete privacy trainings.	Inquired IDEAs Senior Product Manager and IDEAs Principal Program Manager to understand the training requirements for accessing datasets managed by IDEAs.	No exceptions noted.

CO-BO-6.1			
Controls must provide reasonable assurance in preventing unauthorized access to datasets managed by IDEAS.			
Reference	**Control description**	**Test procedures**	**Observations**
		Obtained and inspected evidence of training requirements for access to datasets containing EUPI or OII. Obtained and inspected an audit log to determine completion of training is checked and logged when access to IDEAs datasets is requested.	
CBO6.2	Requests for access to IDEAs datasets are submitted and approved prior to provisioning user, group or non-human account access.	Inquired IDEAs Senior Product Manager and IDEAs Principal Program Manager to understand the process of gaining access to IDEAs datasets including request, privacy review and approval. Obtained and inspected evidence to determine users (non-IDEAs team members) who need access to datasets, need to create a scenario in order to request access to a specific dataset/ report.	No exceptions noted.

CO-BO-6.1			
Controls must provide reasonable assurance in preventing unauthorized access to datasets managed by IDEAS.			
Reference	**Control description**	**Test procedures**	**Observations**
		Obtained and inspected evidence to determine a privacy review approval is required if the requested scenario contains EUPI or OII. Obtained and inspected evidence to determine an IDEAs team member will triage the submitted request to verify if requirements have been met and approve (or deny) the request. For all scenario requests in the audit period, determined if a privacy review was required and approval was documented, and if the scenario was approved by an IDEAs team member.	
CBO6.3	Microsoft requires employees to sign an attestation before accessing datasets.	Inquired IDEAs Senior Product Manager and IDEAs Principal Program Manager to understand the process of attestation for access to datasets. Observed, obtained and inspected evidence to determine users are	No exceptions noted.

CO-BO-6.1

Controls must provide reasonable assurance in preventing unauthorized access to datasets managed by IDEAS.

Reference	Control description	Test procedures	Observations
		required to either specifically acknowledge their existing attestation for a new dataset, or sign a new attestation for that specific dataset, depending on the type of account used. For the scenario access requests in the audit period, determined that the scenario access request as well as the attestation status are logged.	
CBO6.4	Access expires after 90 days.	Inquired IDEAs Senior Product Manager and IDEAs Principal Program Manager to understand the validity period of access granted. Obtained and inspected evidence to determine user access is programmed to be only granted for 90 days. Obtained and inspected evidence to determine that once the expiration date nears, users receive an e-mail stating that their access is about to expire.	No exceptions noted.

CO-BO-6.1

Controls must provide reasonable assurance in preventing unauthorized access to datasets managed by IDEAS.

Reference	Control description	Test procedures	Observations
		Obtained and inspected evidence to determine that once the 90 days have passed, access is revoked of which the used is informed by email. For one example of an access expiration notification, determine that the expiry date in the logging matches the expiry notification. Determined that new access was requested, which revoked the previous access granted.	
CBO6.5	Individual employee are required to re-attest every 90 days to continue use.	Inquired IDEAs Senior Product Manager and IDEAs Principal Program Manager to understand the validity period of attestations. Obtained and inspected evidence to determine attestation is only valid for 90 days. Obtained and inspected evidence to determine that once the 90 days have	No exceptions noted.

CO-BO-6.1

Controls must provide reasonable assurance in preventing unauthorized access to datasets managed by IDEAS.

Reference	Control description	Test procedures	Observations
		passed, access is revoked and the user is instructed via e-mail to renew the attestation. Obtained and inspected logging to determine for one user that each attestation (since 2021) was only valid for 90 days.	

CO-BO-11.1

Controls must provide reasonable assurance that Microsoft follows strict processes and procedures to evaluate, assess and handle 3rd party legal demands for customer data. These processes and procedures must align to the contractual commitments with Customers concerning protection and disclosure of Customer Data and Personal Data.

Reference	Control description	Test procedures	Observations
CBO11.1	Microsoft performs initial review of legal orders and legally binding requests.	Inquired Assistant General Counsel and Program Manager GRC Global to understand the process of the initial review of legal orders and legally binding requests.	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft. No further exceptions noted.

CO-BO-11.1

Controls must provide reasonable assurance that Microsoft follows strict processes and procedures to evaluate, assess and handle 3rd party legal demands for customer data. These processes and procedures must align to the contractual commitments with Customers concerning protection and disclosure of Customer Data and Personal Data.

Reference	Control description	Test procedures	Observations
		Obtained and inspected evidence to determine that Microsoft has a manual in place with instruction on how to perform reviews on facial validity, including a checklist of items relevant for facial validity. Obtained and inspected evidence to determine that Microsoft has guidelines in place for law enforcement agencies with minimum requirements for all legal process. Obtained and inspected evidence to determine that the person who performed the review (triage) is documented in the CRM system.	
CBO11.2	Microsoft attempts to redirect the law enforcement agency to request data directly from the customer.	Inquired Assistant General Counsel and Program Manager GRC Global to understand the process of attempting	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft.

CO-BO-11.1

Controls must provide reasonable assurance that Microsoft follows strict processes and procedures to evaluate, assess and handle 3rd party legal demands for customer data. These processes and procedures must align to the contractual commitments with Customers concerning protection and disclosure of Customer Data and Personal Data.

Reference	Control description	Test procedures	Observations
		to redirect the law enforcement agency to request data directly from the customer. Obtained and inspected evidence to determine that Microsoft has a manual in place which states that LENS will always attempt to re-direct the law enforcement agency to obtain the information directly from the enterprise customer. Obtained and inspected evidence to determine that Microsoft has guidelines in place for law enforcement agencies that state Microsoft will always re-direct the law enforcement agency to obtain the information from the enterprise itself.	No further exceptions noted.

CO-BO-11.1

Controls must provide reasonable assurance that Microsoft follows strict processes and procedures to evaluate, assess and handle 3rd party legal demands for customer data. These processes and procedures must align to the contractual commitments with Customers concerning protection and disclosure of Customer Data and Personal Data.

Reference	Control description	Test procedures	Observations
		Obtained and inspected evidence to determine that Microsoft has a template in place to attempt redirects, and documents these redirects in CRM.	
CBO11.3	Microsoft performs a legal assessment and review of the legal demand for public sector or enterprise customer data.	Inquired Assistant General Counsel and Program Manager GRC Global to understand the process of performing a legal assessment and review of the legal demand for public sector or enterprise customer data. Obtained and inspected evidence to determine that Microsoft has a manual in place which states that LENS attorney review and approval is needed prior to disclosure. Obtained and inspected evidence to determine that Microsoft performs a legal assessment and review for public	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft. No further exceptions noted.

CO-BO-11.1

Controls must provide reasonable assurance that Microsoft follows strict processes and procedures to evaluate, assess and handle 3rd party legal demands for customer data. These processes and procedures must align to the contractual commitments with Customers concerning protection and disclosure of Customer Data and Personal Data.

Reference	Control description	Test procedures	Observations
		sector or enterprise customer data (for example) in case law enforcement refuses to redirect, and documents the outcome.	
CBO11.4	Microsoft challenges the government request for public sector or enterprise customer data where there is a lawful basis for doing so.	Inquired Assistant General Counsel and Program Manager GRC Global to understand the process of challenging the government request for public sector or enterprise customer data where there is a lawful basis for doing so. Obtained and inspected evidence to determine that Microsoft has contractually agreed to challenge legal orders and legally binding requests for enterprise clients and public bodies disclosure. Obtained and inspected evidence to determine that in case of a lawful basis	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft. No further exceptions noted.

CO-BO-11.1

Controls must provide reasonable assurance that Microsoft follows strict processes and procedures to evaluate, assess and handle 3rd party legal demands for customer data. These processes and procedures must align to the contractual commitments with Customers concerning protection and disclosure of Customer Data and Personal Data.

Reference	Control description	Test procedures	Observations
		for doing so, Microsoft challenges a government request for public sector or enterprise customer data.	

CO-BO-11.2

Controls must provide reasonable assurance that the Microsoft LENS team is sufficiently qualified and ensures appropriate skills and competences to handle complex legal orders or requests.

Reference	Control description	Test procedures	Observations
CBO11.5	Microsoft trains the response team appropriately.	Inquired Assistant General Counsel, Senior Director Operations Fulfillment and Program Manager GRC Global to understand the process of training the response team. Obtained and inspected evidence to determine that Microsoft trains the LENS team to be aware regarding security, privacy and compliance.	No exceptions noted.

CO-BO-11.2

Controls must provide reasonable assurance that the Microsoft LENS team is sufficiently qualified and ensures appropriate skills and competences to handle complex legal orders or requests.

Reference	Control description	Test procedures	Observations
		Obtained and inspected evidence to determine that Microsoft maintains a list containing mandatory trainings for the LENS Response Specialists. Obtained and inspected evidence to determine that team managers monitor the completion of the mandatory trainings and that the LENS team members are compliant on mandatory trainings.	
CBO11.6	Microsoft response team has appropriate qualifications.	Inquired Assistant General Counsel, Senior Director Operations Fulfillment and Program Manager GRC Global to understand the qualifications of the response team. Obtained and inspected evidence to determine that the Microsoft LENS	No exceptions noted.

CO-BO-11.2

Controls must provide reasonable assurance that the Microsoft LENS team is sufficiently qualified and ensures appropriate skills and competences to handle complex legal orders or requests.

Reference	Control description	Test procedures	Observations
		team defined required qualifications for LENS attorneys Obtained and inspected evidence to determine that LENS attorneys meet the required qualifications.	
CBO11.7	There are different teams assigned to US-based requests and EU-based requests.	Inquired Assistant General Counsel, Senior Director Operations Fulfillment and Program Manager GRC Global to understand the process of assigning different teams to US-based requests and EU-based requests. Obtained and inspected evidence to determine that Microsoft has a manual and processing guidelines in place describing that requests from the EU/ EEA are handled within the same region.	No exceptions noted.

CO-BO-11.2

Controls must provide reasonable assurance that the Microsoft LENS team is sufficiently qualified and ensures appropriate skills and competences to handle complex legal orders or requests.

Reference	Control description	Test procedures	Observations
		Obtained and inspected evidence to determine that Microsoft has different queues in place to separate EU/ EEA requests from US requests.	

CO-BO-12.1

Controls must provide reasonable assurance that the LENS team follows and maintains processes and systems to manage requests for enterprise data, which prevent disclosing data without Attorney approval and enable data residency during case handling.

Reference	Control description	Test procedures	Observations
CBO12.1	Microsoft protects Customer Data during the review process.	Inquired Assistant General Counsel, Senior Director Operations Fulfillment and Program Manager GRC Global to understand the process of protecting Customer Data during the review process. Obtained and inspected evidence to determine that Microsoft has a manual in place to protect Customer Data as	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft. No further exceptions noted.

CO-BO-12.1

Controls must provide reasonable assurance that the LENS team follows and maintains processes and systems to manage requests for enterprise data, which prevent disclosing data without Attorney approval and enable data residency during case handling.

Reference	Control description	Test procedures	Observations
		part of the attorney review process to ensure demands are specific. Obtained and inspected evidence to determine that if the requested data is available, the data is stored in region until approved for disclosure.	
CBO12.2	Microsoft does not disclose without approval.	Inquired Assistant General Counsel, Senior Director Operations Fulfillment and Program Manager GRC Global to understand the process of disclosure after approval. Obtained and inspected evidence to determine that Microsoft has a manual in place which states that LENS attorney review and approval is needed prior to disclosure. Obtained and inspected evidence to determine that Microsoft does not disclose pulled or preserved data	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft. No further exceptions noted.

CO-BO-12.1

Controls must provide reasonable assurance that the LENS team follows and maintains processes and systems to manage requests for enterprise data, which prevent disclosing data without Attorney approval and enable data residency during case handling.

Reference	Control description	Test procedures	Observations
		impacting enterprise accounts without an approval from a LENS attorney.	

CO-BO-12.2

Controls must provide reasonable assurance that systems in use by LENS to manage and fulfill requests, are subject to Identity and Access (IDA) mechanisms. These IDA mechanisms enable segregation of duties and management oversight, and prevent disclosing data without formal approval.

Reference	Control description	Test procedures	Observations
CBO12.3	Access to case management systems are controlled.	Inquired Security Officer, System Security Architect, Senior Director Operations Fulfillment and Program Manager GRC Global to understand the process of controlled access to case management systems. Obtained and inspected evidence to determine that access to Customer Records Management is restricted to appropriate personnel only.	Exception noted. We determined that the control is designed and implemented by Microsoft. The operating effectiveness could not be evidenced by Microsoft, due to sensitivity of the policies and procedures related to legal orders and legally binding requests. No further exceptions noted.

CO-BO-12.2

Controls must provide reasonable assurance that systems in use by LENS to manage and fulfill requests, are subject to Identity and Access (IDA) mechanisms. These IDA mechanisms enable segregation of duties and management oversight, and prevent disclosing data without formal approval.

Reference	Control description	Test procedures	Observations
		Observed during the meeting that inappropriate personnel does not have access to the case management system. Observed during the meeting to determine that the system requires users to authenticate with 2FA.	
CBO12.4	Access to case handling systems are controlled.	Inquired Security Officer, System Security Architect, Senior Director Operations Fulfillment and Program Manager GRC Global to understand the process of controlled access to case management systems. Obtained and inspected evidence to determine that access to the Compliance Portal is restricted to appropriate personnel only.	Exception noted. We determined that the control is designed and implemented by Microsoft. The operating effectiveness could not be evidenced by Microsoft, due to sensitivity of the policies and procedures related to legal orders and legally binding requests. No further exceptions noted.

CO-BO-12.2

Controls must provide reasonable assurance that systems in use by LENS to manage and fulfill requests, are subject to Identity and Access (IDA) mechanisms. These IDA mechanisms enable segregation of duties and management oversight, and prevent disclosing data without formal approval.

Reference	Control description	Test procedures	Observations
		Observed during the meeting to determine that the system requires users to authenticate with 2FA. Observed during the meeting to determine that users need to authenticate with 2FA through Torus to request access to a corporate product group (Teams).	
CBO12.5	Access to case management and handling systems require management oversight.	Inquired Security Officer, System Security Architect, Senior Director Operations Fulfillment and Program Manager GRC Global to understand the process of management oversight on access to case management and handling systems. Obtained and inspected evidence to determine that all access requests for Customer Records Management (CRM) must be approved by a manager.	Exception noted. We determined that the control is designed and implemented by Microsoft. The operating effectiveness could not be evidenced by Microsoft, due to sensitivity of the policies and procedures related to legal orders and legally binding requests. No further exceptions noted.

CO-BO-12.2

Controls must provide reasonable assurance that systems in use by LENS to manage and fulfill requests, are subject to Identity and Access (IDA) mechanisms. These IDA mechanisms enable segregation of duties and management oversight, and prevent disclosing data without formal approval.

Reference	Control description	Test procedures	Observations
		Obtained and inspected evidence to determine that all access requests for the Compliance Portal must be approved by a manager. Obtained and inspected evidence to determine that granted access is reviewed at least annually by a manager for users to retain access to Customer Records Management (CRM) and the Compliance portal.	

CO-BO-13.1

Controls must provide reasonable assurance that the Microsoft LENS team supports transparency reporting and prevent overdisclosure, by tracking, monitoring and logging all activities during case handling and data disclosure.

Reference	Control description	Test procedures	Observations
CBO13.1	Activities in case management and handling systems are logged.	Inquired Security Officer, System Security Architect, Senior Director Operations Fulfillment, Senior Software	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft.

CO-BO-13.1

Controls must provide reasonable assurance that the Microsoft LENS team supports transparency reporting and prevent overdisclosure, by tracking, monitoring and logging all activities during case handling and data disclosure.

Reference	Control description	Test procedures	Observations
		Engineering Manager and Program Manager GRC Global to understand the process of logging activities in case management and handling systems. Obtained and inspected evidence to determine that actions in CRM are logged in the audit history. Obtained and inspected evidence to determine that actions in Compliance Portal are logged in the audit history. Obtained and inspected evidence to determine logging and event information from both systems are linked through an identifier.	No further exceptions noted.
CBO13.2	Microsoft logs and monitors data extraction.	Inquired Security Officer, System Security Architect, Senior Director Operations Fulfillment, Senior Software Engineering Manager and Program	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft.

CO-BO-13.1

Controls must provide reasonable assurance that the Microsoft LENS team supports transparency reporting and prevent overdisclosure, by tracking, monitoring and logging all activities during case handling and data disclosure.

Reference	Control description	Test procedures	Observations
		Manager GRC Global to understand the process of logging and monitoring of data extraction. Obtained and inspected evidence to determine that actions in Compliance Portal are logged in the audit history.	No further exceptions noted.
CBO13.3	Microsoft logs all disclosures.	Inquired Security Officer, System Security Architect, Senior Director Operations Fulfillment, Senior Software Engineering Manager and Program Manager GRC Global to understand the process of logging disclosures. Obtained and inspected evidence to determine that disclosure of data packages is logged in the law enforcement portal. Obtained and inspected evidence to determine that the package name	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft. No further exceptions noted.

CO-BO-13.1

Controls must provide reasonable assurance that the Microsoft LENS team supports transparency reporting and prevent overdisclosure, by tracking, monitoring and logging all activities during case handling and data disclosure.

Reference	Control description	Test procedures	Observations
		includes the identifier that relates to the legal request.	

CO-BO-13.2

Controls must provide reasonable assurance to prevent overdisclosure and make sure data is minimized to what is compelled and responsive to the request.

Reference	Control description	Test procedures	Observations
CBO13.4	Data extraction is minimized.	Inquired Security Officer, System Security Architect, Senior Director Operations Fulfillment, Senior Software Engineering Manager and Program Manager GRC Global to understand the process of minimizing data extraction. Obtained and inspected evidence to determine that response Specialists pull data through the Compliance Portal.	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft. No further exceptions noted.

CO-BO-13.2

Controls must provide reasonable assurance to prevent overdisclosure and make sure data is minimized to what is compelled and responsive to the request.

Reference	Control description	Test procedures	Observations
		Obtained and inspected evidence to determine that data is pulled by use of specified identifiers.	
CBO13.5	Microsoft minimizes data to what is compelled to disclose and is responsive to the request.	Inquired Security Officer, System Security Architect, Senior Director Operations Fulfillment, Senior Software Engineering Manager and Program Manager GRC Global to understand the process of minimizing data to what is compelled to disclose and being responsive to the request. Obtained and inspected evidence to determine that Response Specialists perform additional cropping of the (preserved) data in accordance with the legal demand.	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft. No further exceptions noted.
CBO13.6	Approved and minimized data packages are only disclosed through a protected environment.	Inquired Security Officer, System Security Architect, Senior Director Operations Fulfillment, Senior Software Engineering Manager and Program Manager GRC Global to understand the	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft. No further exceptions noted.

CO-BO-13.2

Controls must provide reasonable assurance to prevent overdisclosure and make sure data is minimized to what is compelled and responsive to the request.

Reference	Control description	Test procedures	Observations
		process of disclosing approved and minimized data packages through a protected environment. Obtained and inspected evidence to determine that Response Specialists share cropped and encrypted datasets (packages) through a protected Law Enforcement portal. Obtained and inspected evidence to determine that data packages are made available for two weeks and allow a maximum of three download attempts. Obtained and inspected evidence to determine that the Law Enforcement portal is protected.	
CBO13.7	Microsoft has detective controls applicable to data disclosures.	Inquired Security Officer, System Security Architect, Senior Director Operations Fulfillment, Senior Software Engineering Manager and Program	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft.

CO-BO-13.2

Controls must provide reasonable assurance to prevent overdisclosure and make sure data is minimized to what is compelled and responsive to the request.

Reference	Control description	Test procedures	Observations
		Manager GRC Global to understand the process of detective controls applicable to data disclosures. Obtained and inspected to determine that Microsoft has policies and procedures in place to assess a potential over-disclosure. Obtained and inspected to determine that Microsoft has policies and procedures in place to remediate over-disclosure.	No further exceptions noted.

Appendix 2: Additional Information provided by Microsoft

1.1 Legitimate Business Operations: Legal Obligations

Microsoft must be able to show financial and legal compliance with many laws and regulations around the world each year. We must also be able to demonstrate to our customers that we, as their service provider, are fulfilling our obligation to comply with applicable laws and regulations.

In respect to Microsoft Legal Obligations related to government demands for data:

- Consistent with our contractual commitments to our customers, Microsoft does not provide any government with direct or unfettered access to our customers' data, and we do not provide any government with our encryption keys or the ability to break our encryption
- If a government seeks customer data, it must follow applicable legal process. It must serve us with a warrant or equivalent court order for content, or a subpoena or court order for subscriber information or other noncontent data
- Microsoft's legal compliance team reviews all requests to ensure they are valid, rejects those that are not valid, and only provides the data specified in and required by the order

Microsoft's processing of specific legal demands is subject to legal privilege, which must be maintained.

As part of Microsoft's commitments, Microsoft is prohibited from allowing third party access to customer data or to legally privileged information. The rules of engagement mutually agreed before the audit, therefore set necessary limitations on the information that can be shared through the validation process. This included the scope which was defined to the services provided to the Dutch Ministry of Justice within the agreed audit period. During the period under review no relevant legal requests were received by Microsoft related to the Dutch Ministry of Justice, therefore the population sample for legal requests was zero. The lack of a legal demand within scope of the audit does not in any way equate to lack of control or failure to maintain effective controls related to Microsoft's processing of legal demands. It merely indicates that such effectiveness testing was not possible as the population size was zero.

Microsoft provided EY auditors with extensive non-privileged evidence related to our handling of legal demands, including but not limited to (i) direct access to senior members of the Law Enforcement and National Security (LENS) team; (ii) manuals and guidelines that detail our principles, practices, and policies; (iii) excerpted materials illustrating various stages of LENS' handling of relevant legal demands; and (iv) walkthroughs, screenshots, and other evidence related to the case records management system and other technical tools and systems used by the LENS team to respond to lawful access requests.

1.2 Management's response to exceptions identified

The table below contains Management's responses to the exceptions identified:

Control descriptions	Exceptions identified	Management responses
CBO 1.1 **Description:** **Microsoft has centralized privacy policies, standards, and data handling documentation that are reviewed at least annually.**	Per inquiry of the M365 Privacy Program Owner and the M365 Privacy Architect and inspection of documentation an annual review of the Microsoft privacy standards and data taxonomy is in place. Per inquiry of the M365 Privacy Program Owner and the M365 Privacy Architect we were informed that there is no process in place for annual review and approval of the Data Handling Standards by the Microsoft Customer Data Governance Board. Per inquiry of the M365 Privacy Program Owner and the M365 Privacy Architect and per inspection of e-mail conversations and meeting minutes we determined that ~~we were informed that~~ the content of the Data Handling Standards is frequently discussed during the weekly meetings of the Privacy teams, limiting the risk of these document becoming outdated. Moreover, per inquiry of the M365 Privacy Program Owner and the M365 Privacy Architect we were informed that the Data Handling Standards are used daily by a large number of Microsoft employees and are rarely subject to change.	Microsoft acknowledges this observation, but classifies this as a low risk, as Microsoft has implemented policies and procedures to ensure that reviews are undertaken regularly as detailed in the observation. Microsoft has taken action to formalize the annual review of the Data Handling Standards.
CBO 2.2 **Description:** **Microsoft periodically evaluates data processing for products or features**	For one (1) of the seven (7) selected features released during our audit period we determined that one required task in the privacy review, Data Profile, was closed without being executed, due to a human error.	Microsoft acknowledges the observation, but employed compensating controls to address the risk. The exception noted occurred during a system change. As part of the transition to the new systems,

Control descriptions	Exceptions identified	Management responses
through a privacy review. These privacy reviews assess System Generated Logs data flows.	Per inquiry of the Privacy Program Owner for Office 365 and Intelligent Services and per inspection of the Privacy Review and associated evidence we determined that a privacy review was performed for this feature.	Microsoft has ensured that all privacy reviews are completed and approved.
CBO 4.1 **Description:** **Data published in IDEAs reports must undergo a privacy review to ensure that the use of personal data is appropriate, and that data being published is at an appropriate level of aggregation.**	For six (6) of the six (6) selected IDEAs reports in which data was published during the audit, we were not able to determine that a Privacy Review was completed prior to processing and publishing the data in the IDEAs report since there is no technical gate that will prevent an approved user within IDEAs from processing and publishing data without a Privacy Review. For six (6) of the six (6) selected IDEAs reports we determined that a Privacy Review was completed. Per inquiry of the Senior Privacy Product Manager, we were informed that Microsoft has implemented multiple layers of defense including access control, embedded Privacy Champs, and multiparty reviews to mitigate the risk that data may be processed and published in IDEAs reports without the completion of a Privacy Review.	Microsoft acknowledges the observation that there is no technical gate that enforces the requirement of a privacy review. As detailed in the exception, MSFT has already implemented a defense in depth strategy to address this. As such, Microsoft does not plan to make any modification to its existing policies, processes and procedures due to the mitigations already documented.
CBO 11.1, 11.2, 11.3, 11.4 **CBO 12.1, 12.2** **CBO 13.4, 13.5, 13.6, 13.7** **Descriptions: see Appendix 1, table section 1.3**	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft.	Per the context Microsoft outlined above (section 2.1), we were unable to demonstrate the operational effectiveness of these controls as the population size was zero.

Control descriptions	Exceptions identified	Management responses
CBO 12.3, 12.4, 12.5 **Descriptions: see Appendix 1, table section 1.3**	The operating effectiveness could not be evidenced by Microsoft, due to sensitivity of the policies and procedures related to legal orders and legally binding requests.	Microsoft demonstrated access control is an automatic control integrated in case management and handling systems, which were configured to be enabled during the audit period. Microsoft provided a sample which demonstrated the control was operational. Per the context Microsoft outlined above (section 2.1), mutually agreed rules of engagement set necessary limitations on further sharing of information.
CBO 13.1, 13.2, 13.3 **Descriptions: see Appendix 1, table section 1.3**	Non-occurrence since no legal orders nor legally binding requests were received related to participants of SLM Rijk during the audit period, as confirmed by Microsoft. No further exceptions noted.	Microsoft demonstrated logging and monitoring are automatic controls integrated in case management and handling systems, which were configured to be enabled during the audit period. Microsoft demonstrated the control was operating adequately through a sample of the generated logs. Per the context Microsoft outlined above (section 2.1), we were unable to demonstrate the operational effectiveness of these controls as the population size was zero.