# Ministry of Justice and Security

## Assurance report on profiling restrictions with regard to Microsoft's Office 365 ProPlus

From 1 July 2020 to 30 September 2020

Building a better working world

Ernst & Young Accountants LLP
Wassenaarseweg 80
2596 CZ Den Haag, Netherlands
Postbus 90636
2509 LP Den Haag, Netherlands

Tel: +31 88 407 10 00
Fax: +31 88 407 41 87
ey.com

VERTROUWELIJK
Ministerie van Justitie en Veiligheid
T.a.v. de heer P.J.G. van den Berg
Postbus 20301
2500 EH DEN HAAG

Den Haag, 17 maart 2021 REQ5267448-A/DW/ib

## Assurance-rapportage dataprotectie Microsoft MBSA-amendement Rijksoverheid

Geachte heer Van den Berg,

U heeft ons gevraagd om een audit uit te voeren naar de mate van dataprotectie van persoonsgegevens bij Microsoft en in het bijzonder hoe Microsoft zorgt dat profilering van persoonsgegevens wordt voorkomen. Conform ons voorstel van 4 december 2019 met het kenmerk 1010034055 hebben wij de audit uitgevoerd.

In de bij deze brief bijgesloten assurance-rapportage, die conform uw verzoek Engelstalig is opgesteld, geven wij onze conclusies en belangrijkste constatering van de door ons uitgevoerde auditwerkzaamheden. De audit is conform het met u afgestemde controleraamwerk uitgevoerd zoals in de bijlage van de assurance-rapportage is opgenomen.

Onze constateringen in bijgaande assurance-rapportage zijn in het kader van hoor en wederhoor op 18 februari 2021 met Microsoft afgestemd.

Indien u dat wenst, zijn wij graag bereid tot het geven van een nadere (mondelinge) toelichting.

Met vriendelijke groet,
Ernst & Young Accountants LLP

w.g. drs. M.M.J.M. (Marc) Welters RE RA
Partner

# Assurance report of the independent IT Auditor

To: Ministry of Justice and Security – Strategic Vendor Management Microsoft

## Our opinion

We have examined Microsoft's description of controls as included in appendix 1 to the assurance report relating to the personal data protection in Office 365 ProPlus with regard to profiling restrictions as agreed in the agreement (MBSA) and amendments between the Ministry of Justice and Security and Microsoft Corporation (hereafter Microsoft), throughout the period from 1 July 2020 to 30 September 2020. 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 in all material respects:

- the description of controls in appendix 1 fairly presents the controls that were designed and implemented throughout the period from 1 July to 30 September 2020;
- 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 July to 30 September 2020;
- the controls tested operated effectively to achieve the control objectives throughout the period from 1 July to 30 September 2020.

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 opinion

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).

We believe that the assurance evidence we have obtained is sufficient and appropriate to provide a basis for our 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, including, if applicable, the complementary user entity controls assumed in the design of the service organization's controls;
- 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 a subservice organization (inclusive method) or the controls of the service organization to monitor the effectiveness of controls at the subservice organization (carve-out method);
- The description of controls in appendix 1 includes relevant details of changes to controls throughout the period from 1 July to 30 September 2020;
- 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, along with, if applicable, the complementary user entity controls assumed in the design of the service organization's controls, 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 July to 30 September 2020.

## Matters related to the scope of our examination

We have included our scope limitations in appendix 1.

### Complementary user entity controls

The description of controls in appendix 1 indicates that certain control objectives can be achieved only if complementary user entity controls assumed in the design of Microsoft's controls are suitably designed and operating effectively, along with related controls at Microsoft. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls. We have included the relevant complementary user entity controls in appendix 2.

Our opinion is not modified in respect of these matters.

## Limitations of a description and to controls at a service organization

The control objectives are specified by Microsoft and may not, therefore, include every aspect of Microsoft's Office 365 ProPlus services that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. 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 a service organization may become ineffective.

## Restrictions on use and distribution

Our assurance report and this summary are intended solely for the information and for the Ministry of Justice and Security – Strategic Vendor Management Microsoft (SLM Rijk) and their user entities that make use of the services of Microsoft for Office 365 ProPlus during some or all of the period from 1 July 2020 to 30 September 2020, and their (IT) auditors, who have a sufficient understanding to consider our assurance report and this summary, including information about controls not included in this report, that are for user entities themselves, when assessing the risks of material errors or omissions for these user entities.

If and insofar as you are required by law or regulation to disclose our assurance report and this summary to third parties (including the members of the House of Representatives), or if you are otherwise permitted to disclose our report, you must disclose the report as a whole and not in parts. Accordingly, when you disclose the assurance report and summary to third parties, you should advise those third parties that they should consider the assurance report and summary in its entirety.

## Responsibilities of management of the service organization

Microsoft's management is responsible for:

- preparing the description of controls in appendix 1 and 2 and fairly presenting the controls as designed and implemented relating to the Office 365 ProPlus in accordance with the applicable criteria;
- providing Office 365 ProPlus;
- 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's management 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 Control 1 (ISQC 1), 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 and 2 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 July to 30 September, 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 2 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.

The Hague, 17 March 2021

Ernst & Young Accountants LLP

signed by M.M.J.M. Welters
Partner

# Appendix 1

The following is included in this appendix:
1. Control environment
2. Scope
3. Definitions
4. Testing of Information Produced by the Entity
5. Control framework, testing procedures and results

## 1 Control environment

The control environment in this appendix represents a set of controls that is prepared specific to the scope of this engagement but represents controls that are part of the control environment of Microsoft. In planning the nature, timing and extent of our testing of the controls specified in this appendix, we considered the following aspects of Microsoft's control environment: organizational structure, policies and procedures, risk assessment processes and management monitoring procedures.

The privacy and profiling controls that are included in this appendix follow the life cycle of personal data (see figure). This lifecycle provides a view of the lifecycle of personal data from the perspective of the Controller.

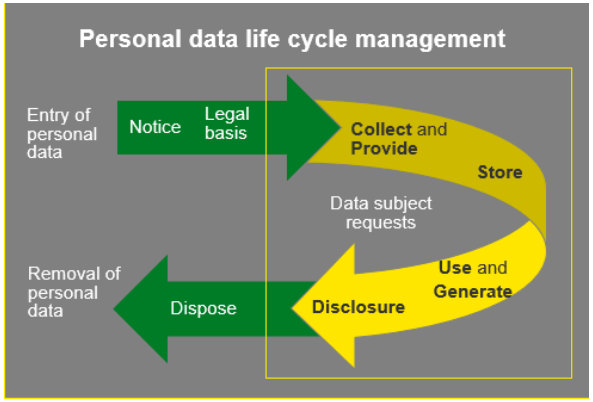


*Figure: Lifecycle of personal data*

The life cycle steps, profiling risk, audit criteria, control activity and control description have been specified as part of our engagement and are aligned with both Microsoft and the Ministry of Justice and Security – Strategic Vendor Management Microsoft.

# 2 Scope

We have performed the audit in line with the engagement letter of 4 december 2019 with the identification '1010034055'. The scope of the audit concerns Microsoft's controls, both in design and operating effectiveness, to adhere to profiling restrictions in accordance with the contract and amendments between Microsoft and the Ministry of Justice and Security in the use of Microsoft Office 365 ProPlus for business on Windows 10.

### Products and services in scope

The products and services in scope concern those that are part of Office365, used by or on behalf of the Dutch government. The following Microsoft products and services are in scope:

- Microsoft Office 365 ProPlus for business on Windows 10 – applying Windows security settings for Windows 10 as advised by Microsoft (these settings are considered as user organization controls). Office365 for Mobile use and for Mac is not in scope.
- Controller Connected Services by Microsoft, that Microsoft Office 365 ProPlus makes use of are not in scope, as the Controller Connected Services are expected be turned off, as reporting in the Data Privacy Impact Assessment (DPIA). Therewith, such is a user organization control. If feasible, we will include

a degree of data collection for the Controlled Connected services in our data analytics procedures as part of phase D, to verify if the service is indeed turned off and no data is collected by Microsoft with regard to connected services.
- Third party services are included, that Microsoft Office 365 Pro Plus provides to users, are expected to be turned off at tenant level (user organization control).

### User organization controls as precondition for the audit

As mentioned above, to comply with some of the criteria to mitigate risks with regard to profiling restrictions, not only Microsoft but also the user organization is to perform control activities. The relevant user organization controls are included in appendix 2.

### Context of audit criteria and control activities

The audit criteria and control activities cover the following topics:
- Risk assessment of profiling of personal data subjects
- Internal policies, guidelines and instructions to ensure compliance regarding profiling
- Designed controls and operating effectiveness of controls
- Monitoring of compliance
- Evaluating compliance
- Reporting of compliance
- Responding to potential non-compliance

In practice the scope of the relevant audit criteria and control activities concerns three areas:
- Privacy and Profiling controls
- Security and Access controls
- Entity level controls

As the Ministry of Justice & Security requested EY to focus the audit on profiling restrictions, we focused our audit activities on *Privacy and Profiling* controls. In some cases we still consider *Security and Access* controls, or *Entity level* controls relevant. In these cases we refer to these areas. Assurance with regard to *Security and Access controls*, as well as *Entity level controls*, are expected to be more generic, and it is expected that assurance for these controls can be obtained by the Ministry of Justice and Security from current SOC 2 reporting that Microsoft already has available. Therefore, this report does not provide assurance related to *Security and Access controls,* as well as *Entity Level controls.*

SOC reports

Microsoft uses general IT processes and has evaluated these processes in various SOC reports. The description of controls in appendix 1 includes only control objectives and related controls of Microsoft specific to profiling of personal information and excludes the control objectives and related controls of general IT processes that are evaluated in the SOC reports. Our examination did not extend to controls of the general IT processes that are included in the SOC reports, and we have not evaluated the suitability of the design or operating effectiveness of such controls. If a control relies (partly) on the SOC reports we have made this explicit in a note.

# 3 Definitions

Microsoft applies the following terminology with regard to personal data:

- **Profiling and Profiles**: As part of this audit, references to "profiling" and "profiles" associated with an online services concern data processing that result in computation of inferences (deductions) or insights about a natural person, that are persisted over time, which would be the only way the inferences could be used as part of automated decisions. These profiling and profiles may be relevant to Controller as part of GDPR, in case these affect the rights and freedoms of individuals.
- **Controller:** Dutch Government's entity managing an Office 365 instance.
- **Processor:** Microsoft Corporation.
- **Personal Data:** personal data as defined in Article 4 of the GDPR.
- **Collect**: Verb defining the data that is obtained by Microsoft via locally running software in the customers environment. This data is called diagnostic data and may contain personal data.
- **Provide:** Verb defining data that is obtained by Microsoft with controller's intent that the data is processed by Microsoft as the controller uses the online services. This data is called Customer Data and will contain personal data.
- **Generate:** Verb defining data that is computed and stored at Microsoft as a result of the operations of the online services for the customer. May contain personal data.
- **Operable controls**: Configuration settings provided by Microsoft, to determine how the service operates.
- **Sub processors**: Other processors as well as Microsoft affiliates, used by Microsoft to process Customer Data and Personal Data in the context of delivering Online Services for which Microsoft is a data processor, as described in Article 28 of the GDPR. Sub processors may have access to or be provided customer data or personal data. Sub processors are a subset of the population of Microsoft's suppliers.
  Microsoft does not provide EUII to sub processors. Agency or temporary staff (staff augmentation) could have access if they work in our control system.

- **DHS**: Data handling standard.
- **PII**: Personal Identifiable Information.
- **EUII**: End User Identifiable Information.
- **EUPI**: End-User Pseudonymous Information, including diagnostic data.
- **DPIA:** Data Privacy Impact Assessment.

# 4 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 performed 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:

- inspected the source of the information produced by the entity,
- inspected the query, script, or parameters used to generate the information produced by the entity,
- tied data between the information produced by the entity and the source, and/or
- 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.

# 5 Control framework, testing procedures and results

For each step in the personal data life cycle, the aligned control framework, our testing procedures and results are documented.

We applied the life cycle of personal data to determine risks from the perspective of the individual and the controller, as the use of the life cycle supports completeness of risk identification. Please note that Microsoft is a processor with regard to the personal data in scope of this audit.

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| **Life cycle step:** | Notice | | | | |
| **Profiling risk:**<br><br>Audit criteria: | Processor does not operate in accordance with instructions, and as a result Controller or Data subject are not aware of building or using profiles to make automated decisions<br>▸ Towards Controller it is transparent that profiling is in accordance with both the instructions as contracted, as well as online configuration settings<br>▸ Towards data subject, it is transparent what profiling takes place with data subject's personal data. | | | | |
| Microsoft communicates to Controller, the nature and extent of personal data processing. | CTRL9 | M | Microsoft has a procedure in place to communicate the nature and extent of personal data processing to the user organization. | Inquired staff and inspected documentation, and noted that Microsoft communicates the nature and extent of personal data processing to the user organizations through various means of communication.<br><br>Observed related systems, and noted that privacy information is available for enterprise and business customers.<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination):<br>▸ Communication between Microsoft and the user organizations | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| Microsoft instructs its staff via its policies and guidelines (Data Handling Standard) in practices to protect tenants (controller) against non-instructed profiling, in line with agreed contracted clauses. | CTRL10 | M | Microsoft has a procedure in place to instruct its staff via its policies and guidelines based on the Data Handling Standard that is yearly reviewed, and if necessary, revised. | Inquired staff and inspected documentation, and noted that Microsoft has an approved Data Handling Standard (DHS) that includes at least:<br>▸ permitted use of data for different types of data<br>▸ for which usage additional procedures need to be performed or additional measures need to be taken, and which uses of data are prohibited<br>▸ information about permissible actions for storage and transfer of data<br><br>Inspected the DHS, and noted that the DHS is reviewed at least once a year by the Privacy Architect.<br><br>Inquired, and noted that all relevant staff receive training on the (policies and guidelines based on the) DHS upon joining the company and has to be repeated on a yearly basis. Note: see control 12 related to the privacy training. | No deficiencies noted. |
| | CTRL11 | M | Microsoft has a review process for new profiling scenarios; if the scenario is not allowed by contract, it is rejected. | Inquired staff and noted that privacy reviews are performed in case of changes in software, dependent on the nature of personal data being affected (e.g. based on the DHS) and the impact of the customer experience.<br><br>Inquired staff and noted that privacy reviews are expected to be triggered to be performed, if needed, considering:<br>▸ Training of relevant staff<br>▸ Having a privacy driver in every development team<br><br>See control 13 related to personal data protection as part of software development. | No occurrences noted.<br><br>No new profiling scenario under review during the audit period.<br><br>As a result, conditions required for the operation of the control did not occur. Therefore, we performed only design testing and |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | Inspected a sample of privacy reviews, and noted that profiling is addressed, but did not occur in the audited period. | no operating effectiveness testing for this control. |
| Microsoft trains its staff to manage the tenants data (incl. personal data) in conformance with its policies and procedures. For this purpose Microsoft provides documentation (e.g. its engineering Data Handling Standard) and training to its staff | CTRL12 | M | Microsoft trains its relevant staff to be aware regarding to:<br>▸ protecting of personal data including EUPI and organizational identifiable information<br>▸ understanding of their roles and responsibilities related to privacy in general and profiling specifically, including those of privacy drivers and privacy managers (for advising, reporting of suspicious activities, and requesting reviews)<br>▸ reporting suspected misuse | Inquired staff and inspected documentation, and noted that Microsoft trains relevant staff on:<br>▸ topics regarding protection of personal data,<br>▸ roles and responsibilities related to privacy in general and profiling specifically.<br>▸ standards of Business Conduct<br>▸ AI principles<br>▸ the Responsible AI Standard<br>▸ staff responsibilities like reporting and seeking guidance for sensitive uses of AI<br>▸ to report suspected misuse or anything that might cause harm to the customer's data<br><br>This training is to be completed by relevant staff upon joining the company, and is to be repeated on a yearly basis.<br><br>Inquired and noted that for engineers that need privileged access, completeness of training is enforced, as such privileged access only grants access if user completed its (re)training timely.<br>We observed and noted that access to personal data requires a privileged access account, and being eligible to make use of this account, requiring completing of required (re)training, enforced via a programmed control. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | Inquired and noted that for other users the training is also mandatory, and timely completion of training is monitored by their managers.<br>We observed dashboards and noted that the order of magnitude of staff in the HR system that requires training and the number of trained staff in the Training dashboard are similar, considering that differences occur due to changes caused by joiners, leavers, changers, and sickness.<br><br>See control 54, in case of privacy incidents being detected, these are followed-up, and remediated, if needed. | |
| Microsoft prepares personal data protection as part of software development | CTRL13 | M | Microsoft prepares personal data protection as part of software development. | Inquired staff and noted that privacy reviews are performed in case of changes in software, dependent on the nature of personal data being affected (e.g. based on the DHS) and the impact of the customer experience.<br><br>Inquired that privacy reviews are expected to be performed, if needed, considering:<br>▸ Enforcing training of relevant staff<br>▸ Having a privacy driver in every development team<br><br>Inquired staff and inspected documentation, and noted that:<br>▸ Peer reviews are required to be performed before releasing new or updated software<br>▸ In case of an exception of postponing the performing of a peer review, such exception is communicated to both engineer and manager, and a peer review is enforced before releasing new or updated software<br>Observed peer reviews in the online peer review tool, and noted that: | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | ▸ Peer reviews are being performed<br>▸ Privacy bots are being used to prepare privacy-related comments to a reviewer, that are to be resolved before completing the peer review<br><br>Inspected a sample of privacy reviews, and determined that profiling is addressed.<br><br>See control 54, in case of privacy incidents being detected, these are followed-up.<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination):<br>▸ Change management<br>▸ Peer review before going into production<br>▸ Roll-out phasing (from smaller community towards all users) | |
| Left blank on purpose | CTRL14 | | Left blank on purpose [1] | Left blank on purpose | Left blank on purpose |
| Microsoft's development teams and their supervisors identify profiling risks in a timely manner, i.e. via their team's privacy driver (highlighting the need for detailed legal or privacy review), to have such | CTRL15 | M | Each development team has its own privacy driver that is trained and competent to perform this role. | Inquired staff and inspected documentation, and noted that Microsoft has a specific team of privacy managers (also known as privacy drivers).<br><br>Inspected documentation, and noted that the privacy managers are qualified, trained and have relevant certifications. | No deficiencies noted. |

[1] CTRL14 does not exist.

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| software development be evaluated by a specialized review team (performing a legal, trust or privacy review) (control also applies to step 'Use'), to prevent these going to production in absence of appropriate basis to obtain controller's instructions | | | | See control 54, in case of privacy incidents being detected, these are followed-up. | |
| | CTRL16 | M | Each software development is evaluated by a specialized review team before the software development is going to production. | Inquired staff and inspected documentation, and noted that reviews in software development are performed based on the nature of a change, based on the nature of personal data being affected (based on the DHS), and the impact of the customer experience.<br><br>See control 13 related to personal data protection as part of software development.<br><br>See control 54, in case of privacy incidents being detected, these are followed-up. | No deficiencies noted. |
| Microsoft evaluates Privacy risks (including profiling risks) at key development stage gates (pass or decline to next stage) (control also applies to step 'Use') | CTRL17 | M | Microsoft evaluates privacy and profiling risks at key development stage gates. A formal agreement is necessary to move forward to the next stage. | Inquired staff and inspected documentation, and noted that, based on Microsoft's policies:<br>▸ each team has a privacy manager who is to evaluate privacy risks as part of a development team, and<br>▸ privacy reviews are performed by a dedicated privacy team, dependent on the nature of a change, considering the nature of personal data being affected, and the impact of the customer experience<br><br>See control 13 related to personal data protection as part of software development.<br><br>Inspected a sample of privacy-related changes, and noted that the privacy manager was involved and performed reviews and, if formal approval was needed, such was enforced. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| Microsoft communicates legally relevant changes in profiling to Controller. Such communications take place adequately and in advance, with guidance to help Controller prepare for potentially legally significant changes | CTRL18 | M | Microsoft has a process to communicate changes to the Online Services that may be perceived legally relevant by the user organization. In case of a certain legally significant change, Microsoft communicates to user organization. | Inquired staff and inspected documentation, and noted that legally significant changes are defined as major changes and Microsoft has several ways to communicate these changes.<br>Inspected documentation and noted that communication was made available to customer tenants.<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination):<br>▸ communication of changes and updates to the Office365 environment | No deficiencies noted. |
| | CTRL19 | M | Microsoft communicates legally significant changes to engineering teams adequately and in advance. | Interviewed, and noted that:<br>▸ legally significant changes that should be known to engineering, are included in (updates of) the privacy training<br>▸ the DHS is updated in case of legally significant changes<br>▸ compliance champions, who are responsible for compliance within the engineering teams have monthly calls, in which significant changes are communicated. Champions are then responsible for spreading this knowledge within their teams | No deficiencies noted. |
| In case of legally significant changes, or changes that could be perceived disruptive to existing Online Services, Microsoft provides ability for Controller to exercise choice to use new or changed functionality pre-launch, enabling controller to | CTRL20 | M | In case of legally significant changes or changes that could be perceived disruptive to existing Online Services, Microsoft enables the user organization to explicitly instruct by choosing. | Inquired staff and inspected privacy reviews, and noted that privacy reviews are performed in case of relevant changes in software, dependent on the nature of personal data being affected (e.g. based on the DHS) and the impact of the customer experience. These privacy reviews can initiate specific privacy controls, if needed.<br><br>See control 13 related to personal data protection as part of software development. | No occurrences noted: No documentation was required to be updated during the audit period. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| explicitly instruct by choosing | | | | Inquired and noted that no legally significant change occurred during the audit period.<br><br>Observed a sample of existing features that have legally significant impact, and noted that choice was being provided to users to activate these features. | As a result, conditions required for the operation of the control did not occur. Therefore, we performed only design testing and no operating effectiveness testing for this control. |
| **Life cycle step:** Legal Basis<br>**Profiling risk:** No legal basis to profile based on instructions issued by controller<br>Audit criteria: ▸ Controller allows for restricted profiling in accordance with GDPR only ▸ Processor performs profiling in accordance with contract and instructions only (which includes GDPR compliance) | | | | | |
| Microsoft updates or creates Customer (shipped) documentation as part of the change management process, if determined necessary based on trust and legal review, for the processing associated with an online services, e.g. for a feature that results in profiling | CTRL23 | M | As part of the change management process Microsoft performs trust and legal reviews. Based on the outcome, (shipped) Customer documentation is updated. | Inquired staff and inspected privacy reviews, and noted that privacy reviews are performed in case of relevant changes in software, dependent on the nature of personal data being affected (e.g. based on the DHS) and the impact of the customer experience. These privacy reviews can initiate specific privacy controls, if needed, such as updating customer documentation.<br>Inspected documentation and noted that communication was made available to customer tenants.<br><br>See control 13 related to personal data protection as part of software development.<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination): | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | ▸ communication of changes and updates to the Office365 environment | |
| Microsoft adequately in advance notifies Controller, if determined necessary based on trust and legal review, with regard to Microsoft's changes to existing in-production Online Service functionality, i.e. shares its actualized documentation, that is introducing processing associated with an online services feature that results in profiling, if any. Such allows Controller to apply choice with regard to new or changed functionality (consider EY audit activity covering review requests, reviews and need for documentation and notice) | CTRL24 | M | Microsoft adequately in advance notifies user organization, if determined necessary based on trust and legal review, with regard to Microsoft's changes to existing in-production Online Service functionality that is introducing processing associated with an online service feature that results in profiling. | Inquired staff and inspected privacy reviews, and noted that privacy (including trust and legal) reviews are performed in case of relevant changes in software, dependent on the nature of personal data being affected (e.g. based on the DHS) and the impact of the customer experience. These privacy reviews can initiate specific privacy controls, if needed, such as updating customer documentation.<br><br>Inquired and noted that no notification was required during the audit period, based on the outcome of trust and legal reviews.<br><br>See control 13 related to personal data protection as part of software development. | No occurrences noted: No documentation was required to be updated during the audit period.<br><br>As a result, conditions required for the operation of the control did not occur. Therefore, we performed only design testing and no operating effectiveness testing for this control. |
| Microsoft processes personal data only in accordance with operable control settings as set by Controller, allowing Controller to instruct via these settings (consider EY audit activity covering i.e. via admin console, script, SKU selection) | CTRL26 | M | Microsoft processes collected personal data only in accordance with operable control settings as set by user organization, allowing user organization to instruct via these settings. | Inquired staff and inspected privacy reviews, and noted that privacy reviews are performed in case of relevant changes in software, dependent on the nature of personal data being affected (e.g. based on the DHS) and the impact of the customer experience. These privacy reviews can initiate specific privacy controls, if needed, such as operable control settings. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | Observed operable control settings, and noted that user organization can instruct to (de-)activate services, and, if activated, users can also disable such services.<br><br>See control 13 related to personal data protection as part of software development. | |
| **Life cycle step:** Provide and collect<br>**Profiling risk:** Processor receives personal data un-instructed, that could be used for the purpose of profiling<br>Audit criteria: ▸ Processor only receives (provides or collects) personal data that can be used for profiling, as far as instructed | | | | | |
| Microsoft has a Data Handling Standard and trains its staff's awareness and application with regard to categorizing and processing of personal data (i.e. Customer content, EUII, EUPI) accordingly, in line with GDPR | CTRL10 | M | Microsoft has a procedure in place to instruct its staff via its policies and guidelines based on the Data Handling Standard that is yearly reviewed, and if necessary, revised. | Inquired staff and inspected documentation, and noted that Microsoft has an approved DHS that includes at least<br>▸ permitted use of data for different types of data<br>▸ for which usage additional procedures need to be performed or additional measures need to be taken, and which uses of data are prohibited<br>▸ information about permissible actions for storage and transfer of data<br><br>Inspected the DHS, and noted that the DHS is reviewed at least once a year by the Privacy Architect.<br><br>Inquired, and noted that all relevant staff receive training on the (policies and guidelines based on the) DHS upon joining the company and has to be repeated on a yearly basis. Note: see control 12 related to the privacy training. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | CTRL29 | M | Microsoft trains its staff's awareness and application with regard to categorizing and processing of personal data in line with GDPR. | Inquired staff and inspected privacy training documentation, and noted that<br>▸ staff is trained on categorization of data<br>▸ GDPR obligations are included in training<br>▸ DHS is part of privacy training<br>▸ DHS includes permitted use of data for different types of data, including personal data per the GDPR<br><br>Inquired and noted that the privacy training has to be re-trained at least once a year by all relevant employees (see control 12 related to the privacy training). | No deficiencies noted. |
| Microsoft categorizes provided personal data (e.g. EUII, EUPI, Customer Content) by placing such personal data in their designated boundaries. | CTRL30 | M | Microsoft processes collects personal data only in accordance with operable control settings as set by user organization, allowing user organization to instruct via these settings. | Inquired staff and inspected privacy reviews, and noted that privacy reviews are performed in case of relevant changes in software, dependent on the nature of personal data being affected (e.g. based on the DHS) and the impact of the customer experience. These privacy reviews can initiate specific privacy controls, if needed, such as operable control settings.<br><br>Observed operable control settings, and noted that user organization can instruct to (de-)activate services, and, if activated, users can also disable such services.<br><br>See control 13 related to personal data protection as part of software development. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| Microsoft has policies and guidelines to process collected data only for the Purpose as agreed with Controller, as set forth in contract (e.g. the performance of the service, the security of the service and to keep the service up to date, as well as legitimate interests) | CTRL31 | M | Microsoft has policies and guidelines to process collected data only for the Purpose as agreed with user organization, as set forth in contract (e.g. the performance of the service, the security of the service and to keep the service up to date, as well as legitimate interests). | Inquired staff and inspected Online Service Terms (OST) and noted that<br>▸ OST contains instructions on allowable and restricted use of data and specifications of legitimate business operations<br><br>Inquired staff and inspected documentation, and noted that Microsoft has an approved DHS that includes:<br>▸ permitted use of data for different types of data<br>▸ for which usage additional procedures need to be performed or additional measures need to be taken, and which uses of data are prohibited | No deficiencies noted. |
| In order to protect the rights and freedoms of individuals, a risk-based review process exists to evaluate for new features and services. The reviewers may require a necessary and proportional method of customer choice concerning the collection of personal data. | CTRL32 | M | For each feature or/and service, a risk-based review process is carried out. The reviewers may require a necessary and proportional method of customer choice concerning the collection of personal data. | Inquired staff and inspected privacy reviews, and noted that privacy reviews are performed in case of relevant changes (features or services) in software, dependent on the nature of personal data being affected (e.g. based on the DHS) and the impact of the customer experience. These privacy reviews can initiate specific privacy controls, if needed, which may require customer choice concerning the service or functionality.<br><br>See control 13 related to personal data protection as part of software development. | No deficiencies noted. |
| Microsoft categorizes personal data collected via Microsoft software operated by Controller | CTRL33 | M | Microsoft processes collected personal data only in accordance with operable control settings as set by user organization, allowing user organization to instruct via these settings. | Inquired staff and inspected privacy reviews, and noted that privacy reviews are performed in case of relevant changes in software, dependent on the nature of personal data being affected (e.g. based on the DHS and the impact of the customer experience. These privacy reviews can initiate specific privacy controls, such as operable control settings. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | Observed operable control settings, and noted that user organization can instruct to (de-)activate services, and, if activated, users can also disable such services.<br><br>See control 13 related to personal data protection as part of software development. | |
| Microsoft processes collected personal data only in accordance with operable controls as set by Controller, allowing Controller to instruct (i.e. via admin console, script, SKU selection, etc.), as applicable | CTRL33 | M | Microsoft processes collected personal data only in accordance with operable control settings as set by user organization, allowing user organization to instruct via these settings. | Inquired staff and inspected privacy reviews, and noted that privacy reviews are performed in case of relevant changes in software, dependent on the nature of personal data being affected (e.g. based on the DHS) and the impact of the customer experience. These privacy reviews can initiate specific privacy controls, such as operable control settings.<br><br>Observed operable control settings, and noted that user organization can instruct to (de-)activate services, and, if activated, users can also disable such services.<br><br>See control 13 related to personal data protection as part of software development. | No deficiencies noted. |
| **Life cycle step:** | Store | | | | |
| **Profiling risk:** | ▸ Personal data is accessed to build a profile without authorization<br>▸ A data subject's profile is accessed without authorization | | | | |
| Audit criteria: | ▸ Personal data, including profiles, are secured against unauthorized access by known and unknown users (linked to Security and Access)<br>▸ Access to personal data, including profiles, is restricted to authorized users only (refer to Security and Access) | | | | |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| Microsoft has policies and guidelines, e.g. its Data Handling standard, and trains its staff to be aware that data is to be processed in "an environment that meets the policy requirements applicable to its data category (e.g. EUII, EUPI, customer content)" aka "boundary" | CTRL10 | M | Microsoft has a procedure in place to instruct its staff via its policies and guidelines based on the Data Handling Standard that is yearly reviewed, and if necessary, revised. | Inquired staff and inspected documentation, and noted that Microsoft has an approved DHS that includes at least<br>▸ permitted use of data for different types of data<br>▸ for which usage additional procedures need to be performed or additional measures need to be taken, and which uses of data are prohibited<br>▸ information about permissible actions for storage and transfer of data<br><br>Inspected the DHS, and noted that the DHS is reviewed at least once a year by the Privacy Architect.<br><br>Inquired, and noted that all relevant staff receive training on the (policies and guidelines based on the) DHS upon joining the company and has to be repeated on a yearly basis.<br>See control 12 related to the privacy training. | No deficiencies noted. |
| | CTRL34 | M | Microsoft trains its staff to be aware that data is to be processed in an environment that meets the policy requirements applicable to its data category (boundary). | Inquired staff and inspected documentation, and noted that Microsoft trains relevant staff on:<br>▸ topics regarding protection of personal data,<br>▸ existence and use of Microsoft's DHS, which included permissibility of data transmission, data storage and data use<br><br>This training is to be completed by relevant staff upon joining the company, and is to be repeated on a yearly basis.<br>See control 12 related to the privacy training. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| Microsoft stores personal data within the applicable boundary for the asset type (i.e. Customer Content, EUII, EUPI), and consequently in the environment that is in line with the category of such data (consider EY audit activity verifying existing boundaries, categories of personal data, assurance schemes, e.g. SSAE18 SOC boundary , ISO 27701 boundary). | CTRL35 | M | Microsoft processes all generated data in the designated boundaries, for the applicable category of personal data, i.e. EUPI, EUII, Customer Content, unless generated data is anonymized. | Inquired staff and inspected the DHS, covering permissibility of data transmission, data storage and data use, and noted that<br>▸ data cannot be processed in a boundary without having been transported to that boundary<br>▸ allowable transmission between boundaries implicitly covers the processing of data in the correct boundary<br><br>Inquired staff and inspected documentation, and noted that<br>▸ the applicable DHS should always be followed<br>▸ staff privacy training is required before having access to privacy-related data<br>▸ relevant changes to software for collecting and processing of personal data requires a privacy review prior to implementation<br>▸ monitoring and follow-up is in place to verify if EUII would be leaving its boundary<br><br>Observed scrubbing of PII and PII leakage detection, and noted that these automated processes are in place. | No deficiencies noted. |
| Microsoft has means to resolve pseudonymized personal data to identifiable personal data. The additional data necessary for such resolution is only processed within the boundary of Customer data (e.g. hash salts, User Principal Names) | CTRL36 | M | Microsoft has the ability to resolve pseudonymized personal data to identifiable personal data. The additional data necessary for such resolution is only processed within the boundary of Customer data. | Inquired and noted that pseudonymized data can be resolved to identifiable personal data via decryption. Encryption and decryption takes place within the compliance boundary, where the encryption originally was performed.<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination):<br>▸ access to the decryption service within the compliance boundary | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | | |
| Microsoft applies access controls for time-limited access by staff to customer data, i.e. EUII, and Customer content | CTRL37 | M | In case Microsoft staff need access to customer data, i.e. EUII and Customer content, Microsoft staff need to request access and only have time-limited access to customer data. | Per interview we noted that<br>▸ access to the production environment is only granted after manager approval<br>▸ access to customer data, such as EUII and Customer Content, is considered to be higher level access, and this elevated access can be requested and granted through Just In Time (JIT) and time-restricted access, as well as Customer Lockbox access<br><br>We observed and noted that access to personal data requires a privileged access account, and being eligible to make use of this account, requiring completing of required (re)training, enforced via a programmed control.<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination):<br>▸ Just In Time access<br>▸ Customer Lockbox access<br>▸ new and modified user access | No deficiencies noted. |
| Microsoft applies access controls for access by staff to EUPI | CTRL38 | M | Microsoft applies access controls for access by staff to EUPI | Inquired and noted that<br>▸ EUPI data is stored in an internal data store called Cosmos, where data is stored in virtual clusters<br>▸ access to virtual clusters in Cosmos is only possible through the use of a privileged access identity (separate Azure Active Directory)<br>▸ only qualified employees can request a privileged access identity and gain access to virtual clusters in Cosmos. When logged on to Cosmos with their | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | Microsoft identity, users can view the Cosmos catalog but not enter any virtual clusters<br><br>Inquired and inspected documentation, and noted that the qualification process contains the following steps<br>▸ background check (expiring after 740 days)<br>▸ security and privacy training (plus additional training in case user will work with sensitive data)<br>▸ attestation for access to EUPI (expires after 90 days)<br><br>Observed automated controls with regard to access to EUPI, and noted that access is not possible with regular account, and is possible with a privileged access account, also requiring multifactor authentication. After they have logged in, users can select a virtual cluster from the Cosmos 'catalog'. In order to gain access to a virtual cluster, the user has to request an eligibility, for which manager approval is needed. These eligibilities expire every 90 days, after which manager approval needs to be renewed. In case a user does not use the eligibility for 56 days, the eligibility expires (even if the 90 days have not yet passed). | |
| Microsoft encrypts personal data that is in transit between Microsoft operated systems whether remaining inside a compliance boundary or traversing to a different one. | CTRL39 | M | Personal data in transit between Microsoft operated systems is encrypted. | Inquired staff and inspected documentation, and noted three 'in transit' scenarios,<br>▸ between customer and data center<br>▸ between data centers<br>▸ between data centers and Microsoft<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination):<br>▸ the encryption of personal data in transit | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | | |
| **Life cycle step:** | Use and Generate | | | | |
| **Profiling risk:** | ▸ Processor builds or uses profiles not in accordance with contract or instructions of controller<br>▸ As a result of a new or an amended function<br>▸ As part of data analytics<br>▸ Due to privacy violation | | | | |
| Audit criteria: | ▸ Processor only uses profiles for the performance of the service, the security of the service and to keep the service up to date, as well as legitimate interests as far as agreed with controller, in the services' current state and as a result of changes<br>▸ Personal data, including profiles, are secured against unauthorized access by known and unknown users (refer to Security and Access)<br>▸ Access to personal data, including profiles is limited to approved users and for a limited period (refer to Security and Access) | | | | |
| Microsoft has policies and guidelines (i.e. Data Handling Standard) and trains its relevant staff to be aware with regard to:<br>▸ protecting of personal data including EUPI and organizational identifiable information<br>▸ understanding of their roles and responsibilities related to privacy in general and profiling specifically, including those of privacy drivers and privacy managers (for advising, reporting of | CTRL40 | M | Microsoft has policies and guidelines that are annually reviewed and updated where needed regarding:<br>▸ protecting of personal data including EUPI and organizational identifiable information<br>▸ understanding of their roles and responsibilities related to privacy in general and profiling specifically, including those of privacy drivers and privacy managers (for advising, reporting of | Inquired staff and inspected documentation, and noted that Microsoft has an approved DHS that includes guidelines for protection of personal data, including:<br>▸ permitted use of data for different types of data<br>▸ retention times for different types of data<br>▸ for which usage additional procedures need to be performed or additional measures need to be taken, and which uses of data are prohibited<br>▸ information about permissible actions for storage and transfer of data<br><br>Inspected DHS, and noted that DHS is reviewed at least once a year by the Privacy Architect.<br><br>Inquired staff and inspected documentation, and noted that all staff receives training on the (policies and guidelines based on the) DHS and relevant staff on privacy. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| suspicious activities, and requesting reviews)<br>▸ reporting suspected misuse | | | suspicious activities, and requesting reviews)<br>▸ reporting suspected misuse | This training includes roles and responsibilities, as well as guidelines on how to report suspected misuse. | |
| | CTRL12 | M | Microsoft trains its relevant staff to be aware regarding to:<br>▸ protecting of personal data including EUPI and organizational identifiable information<br>▸ understanding of their roles and responsibilities related to privacy in general and profiling specifically, including those of privacy drivers and privacy managers (for advising, reporting of suspicious activities, and requesting reviews)<br>▸ reporting suspected misuse | Inquired staff and inspected documentation, and noted that Microsoft trains relevant staff on:<br>▸ topics regarding protection of personal data,<br>▸ roles and responsibilities related to privacy in general and profiling specifically.<br>▸ standards of Business Conduct<br>▸ AI principles<br>▸ the Responsible AI Standard<br>▸ staff responsibilities like reporting and seeking guidance for sensitive uses of AI<br>▸ to report suspected misuse or anything that might cause harm to the customer's data<br><br>This training is to be completed by relevant staff upon joining the company, and is to be repeated on a yearly basis.<br><br>Inquired and noted that for other users the training is also mandatory, and timely completion of training is monitored by their managers.<br>We observed dashboards and noted that the order of magnitude of staff in the HR system that requires training and the number of trained staff in the Training dashboard are similar, considering that differences occur due to changes caused by joiners, leavers, changers, and sickness. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | See control 54, in case of privacy incidents being detected, these are followed-up, and remediated, if needed. | |
| Microsoft has policies and guidelines (i.e. Data Handling Standard) that require significant changes in processing purposes or processed data to undergo reviews with privacy, security, and/or CELA (Corporate and External Legal Affairs) | CTRL41 | M | Microsoft has policies and guidelines (i.e. Data Handling Standard) that require significant changes in processing purposes or processed data to undergo reviews with privacy, security, and/or CELA (Corporate and External Legal Affairs) | Inquired staff and inspected documentation, and noted that Microsoft has an approved DHS that includes at least:<br>▸ permitted use of data for different types of data<br>▸ retention times for different types of data<br>▸ for which usage additional procedures need to be performed or additional measures need to be taken, and which uses of data are prohibited<br>▸ information about permissible actions for storage and transfer of data<br><br>Inspected DHS, and noted that DHS is reviewed at least once a year by the Privacy Architect.<br><br>Per inspection of documentation we noted that the change management process includes a privacy review. Also we noted per inspection of documentation that security and privacy reviews are pre-requisites for releases. | No deficiencies noted. |
| Microsoft ensures as part of software development:<br>▸ Microsoft's development teams identify profiling risks adequately in advance, (e.g. via their team's privacy driver or privacy manager - | CTRL42 | M | As part of software development Microsoft's development teams identify profiling risks adequately in advance (e.g. via privacy driver) and have such software developments evaluated (DPIA) by a specialized review | Inquired staff and noted that privacy reviews are performed in case of changes in software, dependent on the nature of personal data being affected (e.g. based on the DHS) and the impact on the customer experience.<br><br>Inquired staff and noted that privacy reviews are expected to be performed, if needed, considering:<br>▸ Training of relevant staff | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| highlighting the need for detailed legal or privacy review), have such software development be evaluated (data privacy impact assessment) by a specialized review team (performing a legal, trust or privacy review), to determine if the development meets the requirements related to profiling risks before to move to production<br>▸ Microsoft evaluates computational approaches that could be considered profiling, at key development stage gates (decline, or pass to next stage) | | | team performing a legal, trust or privacy review. | ▸ Having a privacy driver in every development team<br><br>Inspected a sample of privacy reviews, and determined that profiling is addressed.<br><br>Inquired staff and inspected documentation and noted that DPIAs are performed and updated regularly.<br><br>Observed a sample of DPIAs, and noted that:<br>▸ Risks with regard to the rights and freedoms of individuals, including with regard to profiling, are analyzed, and<br>▸ if needed, required controls are reported<br><br>Inquired and inspected overview of DPIAs, and noted that:<br>▸ CELA (Corporate, External, and Legal Affairs) Privacy Management Council maintains DPIAs<br>▸ performance monitoring of updating DPIAs are performed<br>Inquired and inspected DPIA reviews, and noted that samples of DPIA's are reviewed.<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination):<br>▸ Change management<br>▸ Peer review before going into production<br>▸ Roll-out phasing (smaller community towards all users) | |
| | CTRL43 | M | As part of software development Microsoft's development teams determine whether developments meet | Inquired staff and inspected documentation, and noted in case of privacy implications, specific reviews during all development stages are performed by privacy and legal specialists, including specific focus on profiling risks. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | the requirements related to profiling risks before moving to production. | Inspected a sample of privacy reviews during key development stages and noted that privacy specialists were involved and key focus areas were discussed and addressed.<br><br>See control 12 related to the privacy training.<br><br>See control 13 related to personal data protection as part of software development. | |
| | CTRL44 | M | For each key development stage gates Microsoft evaluates computational approaches that could be considered profiling. | Inquired staff and inspected documentation, and noted in case of privacy implications, specific reviews during all development stages are performed by privacy and legal specialists, including specific focus on profiling risks.<br><br>Inspected a sample of privacy reviews during key development stages and noted that compliance experts, privacy experts, legal experts and development representatives were involved. Also we noted that profiling was addressed specifically.<br><br>See control 12 related to the privacy training.<br><br>See control 13 related to personal data protection as part of software development. | No deficiencies noted. |
| Microsoft applies access controls time-based and monitored (i.e. logged), for access by personnel to | CTRL45 | M | Microsoft applies access controls time-based and monitored (i.e. logged), for access by personnel to | Per interview we noted that<br>▸ access to the production environment is only granted after manager approval | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| Customer Data (EUII and Customer content) (refer to Security and Access) | | | Customer Data (EUII and Customer content). | ▸ access to customer data, such as EUII and Customer Content, is considered to be higher level access, and this elevated access can be requested and granted through Just In Time (JIT) and time-restricted access, as well as Customer Lockbox access<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination):<br>▸ Just In Time access<br>▸ Customer lockbox<br>▸ Elevated access | |
| Microsoft processes personal data within their designated boundary, dependent on the category of personal data, i.e. EUII, Customer Content, EUPI | CTRL35 | M | Microsoft processes all generated data in the designated boundaries, for the applicable category of personal data, i.e. EUPI, EUII, Customer Content, unless generated data is anonymized | Inquired staff and inspected the DHS, covering permissibility of data transmission, data storage and data use, and noted that<br>▸ data cannot be processed in a boundary without having been transported to that boundary<br>▸ allowable transmission between boundaries implicitly covers the processing of data in the correct boundary<br><br>Inquired staff and inspected documentation, and noted that<br>▸ the applicable DHS should always be followed<br>▸ staff privacy training is required before having access to privacy-related data<br>▸ relevant changes to software for collecting and processing of personal data requires a privacy review prior to implementation<br>▸ monitoring and follow-up is in place to verify if EUII would be leaving its boundary | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | Observed scrubbing of PII and PII leakage detection, and noted that these automated processes are in place. | |
| Microsoft converts personal data from EUII to EUPI, if being processed by Microsoft in systems outside Customer data boundary (EUII and Customer content) | CTRL46 | M | Microsoft converts personal data from EUII to EUPI, if being processed by Microsoft in systems outside user organization's data boundary (EUII and Customer content). | Inquired staff and inspected documentation and noted that personal identifiable information is removed when data is transferred outside the data boundary.<br><br>Observed the automatic functionality (PII scrubber) that removes personally identifiable information as part of the automatic transferring to outside the boundary.<br><br>Inquired staff and inspected documentation, and noted that a PII leakage detection process is in place and is followed up regularly. | No deficiencies noted. |
| EUII, EUPI and content are encrypted in transit between Microsoft operated systems inside or outside the customer data compliance boundary | CTRL47 | M | EUII, EUPI and content are encrypted in transit between Microsoft operated systems inside or outside the customer data compliance boundary | Inquired staff and inspected documentation, and noted that there are three 'in transit' scenarios<br>▸ between customer and data center<br>▸ between data centers<br>▸ between data centers and Microsoft<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination):<br>▸ the encryption of personal data in transit | No deficiencies noted. |
| Microsoft has a policy that requires to only have software in production, that has been appropriately | CTRL48 | M | Software in production has been appropriately approved for production processing. | Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination): | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| approved for production processing (e.g. as part of change management) | | | | ▸ Approval prior to implementation within the change management process | |
| Microsoft has policies and guidelines and trains its staff to be aware with regard to restrictions on the use and data scopes approved for profiling, e.g. for machine learning based solutions<br>▸ An internal Data Protection Privacy Assessment (DPIA) is performed by Microsoft for in cases where high risk processing of personal data is expected, i.e. when CELA or Privacy Drivers instruct the organization to do so | CTRL40 | M | Microsoft trains its relevant staff to be aware regarding to:<br>▸ protecting of personal data including EUPI and organizational identifiable information<br>▸ understanding of their roles and responsibilities related to privacy in general and profiling specifically, including those of privacy drivers and privacy managers (for advising, reporting of suspicious activities, and requesting reviews)<br>▸ reporting suspected misuse | Inquired staff and inspected documentation, and noted that Microsoft has an approved DHS that includes at least<br>▸ permitted use of data for different types of data<br>▸ for which usage additional procedures need to be performed or additional measures need to be taken, and which uses of data are prohibited<br>▸ information about permissible actions for storage and transfer of data<br><br>Inspected DHS, and noted that DHS is reviewed at least once a year by the Privacy Architect.<br><br>Inquired staff and noted that all staff receives training on the (policies and guidelines based on the) DHS upon joining the company.<br><br>Inquired staff and inspected documentation, and noted that all staff receives training on the (policies and guidelines based on the) DHS and relevant staff on privacy. Note: see control 12 related to the privacy training. | No deficiencies noted. |
| | CTRL49 | M | An internal Data Protection Privacy Assessment (DPIA) is performed by Microsoft for cases where high risk processing of personal data is expected, i.e. when CELA or Privacy Drivers instruct the organization to do so. | Inquired staff and noted that privacy reviews are performed in case of changes in software, dependent on the nature of personal data being affected (e.g. based on the DHS) and the impact on the customer experience.<br><br>Inquired staff and noted that privacy reviews are expected to be performed, if needed, considering:<br>▸ Training of relevant staff | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | ▸ Having a privacy driver in every development team<br><br>Inspected a sample of privacy reviews, and determined that profiling is addressed.<br><br>Inquired staff and inspected documentation and noted that DPIAs are performed and updated regularly.<br><br>Observed a sample of DPIAs, and noted that:<br>▸ Risks with regard to the rights and freedoms of individuals, including with regard to profiling, are analyzed, and<br>▸ if needed, required controls are reported<br><br>Inquired and inspected overview of DPIAs, and noted that:<br>▸ CELA Privacy Management Council maintains DPIAs<br>▸ performance monitoring of updating DPIAs are performed<br>▸ Inquired and inspected DPIA reviews, and noted that samples of DPIA's are reviewed. | |
| Microsoft has and applies a policy for permitted data scopes and data handling in machine learning solutions as part of service features. | CTRL50 | M | Microsoft has and applies a policy for permitted data types and data handling in machine learning solutions as part of service features. | Inquired staff and inspected DHS, covering permissibility of data transmission, data storage and data use, and noted that<br>▸ use of data for machine learning is specifically included in the DHS<br>▸ use of data is part of the review process by privacy managers during software development, in which the DHS is applied | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| Data analytics as part of service: Microsoft applies policies and guidelines (e.g. Data Handling Standard) that require a data scientist to be approved to train a machine learning model, and any access to online service customer data or personal data during development or production operations is consistent with policies (i.e. Data Handling Standard) for access to such data by personnel generally (i.e. model training is eyes off, no access to personal data). | CTRL10 | M | Microsoft has a procedure in place to instruct its staff via its policies and guidelines based on the Data Handling Standard that is yearly reviewed, and if necessary, revised. | Inquired staff and inspected documentation, and noted that Microsoft has an approved DHS that includes at least<br>▸ permitted use of data for different types of data<br>▸ for which usage additional procedures need to be performed or additional measures need to be taken, and which uses of data are prohibited<br>▸ information about permissible actions for storage and transfer of data<br><br>Inspected the DHS, and noted that the DHS is reviewed at least once a year by the Privacy Architect.<br><br>Inquired, and noted that all relevant staff receive training on the (policies and guidelines based on the) DHS upon joining the company and has to be repeated on a yearly basis. Note: see control 12 related to the privacy training. | No deficiencies noted. |
| | CTRL51 | M | Microsoft requires data scientists to be approved to train a machine learning model. Any access to online service customer data or personal data during development or production operations is consistent with the Data Handling Standard for access to such data by personnel generally. | Inquired staff and inspected documentation, and noted that a privacy review is required if creating or training machine learning models.<br><br>Inspected a sample and noted that a privacy review is performed and approved.<br><br>See control 13 related to personal data protection as part of software development. | |
| When performing processing of customer data or personal data for its legitimate business operations (e.g. | CTRL52 | M | Microsoft only processes data already provided to or collected by Microsoft through the use of the online service | Inspected documentation and noted that the contract with user organizations states for which purposes Microsoft may not process the data, such as data analytics, profiling, | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| billing), Microsoft only processes data already provided to, or collected by Microsoft through the use of the online service | | | for its legitimate business operations. | advertising, market research, unless this is authorized in accordance with Customer's documented instructions.<br><br>The contract also states that data may be used for Microsoft's legitimate business operations, to the extent that this does not go beyond billing and preparing invoices; account management; compensation; financial reporting in accordance with legal and stock exchange obligations; revenue metrics; pricing; assessing usage of the Online Services; business planning including structuring its business and branding; product strategy; internal executive reports and capacity modeling and forecasting; improving the core functionality of accessibility, privacy, or energy-efficiency; combatting fraud, cybercrime and cyber-attacks that may affect any Microsoft product or service, not including discretionary scanning of contents of Customer Data or targeting of Customer Users without prior notice to Customer; or complying with Microsoft's legal obligations, subject to the "Disclosure of Customer Data" provision in the Data Protection Terms of the OST and the confidentiality obligations set forth in the MBSA.<br><br>Inspected documentation and noted that the following policies and guidelines are in place with regard to the processing of collected data only for the purposes as agreed with user organization:<br>▸ DHS<br>▸ Access Classification Standard<br><br>Inquired, and noted that all staff receive training on the (policies and guidelines based on the) DHS upon joining the company. | |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | See control 12 related to the privacy training.<br><br>Inquired staff and inspected privacy reviews, and noted that privacy reviews are performed in case of relevant changes (features or services) in software, dependent on the nature of personal data being affected (e.g. based on the Data Handling Standard) and the impact of the customer experience. These privacy reviews can initiate specific privacy controls, if needed, which may require customer choice concerning the service or functionality.<br><br>See control 13 related to personal data protection as part of software development. | |
| Microsoft conducts training for relevant staff, for standards of business conduct, and privacy, to help staff recognize violations, and report violations | CTRL53 | M | Microsoft conducts training for relevant staff, for standards of business conduct, and privacy, to help staff recognize violations, and report violations | Inquired staff and inspected documentation, and noted that Microsoft has an approved DHS that includes at least:<br>▸ Permitted use of data for different types of data<br>▸ for which usage additional procedures need to be performed or additional measures need to be taken, and which uses of data are prohibited<br>▸ information about permissible actions for storage and transfer of data<br><br>Inspected DHS, and noted that DHS is reviewed at least once a year by the Privacy Architect.<br><br>Inquired, and noted that all staff receive training on the (policies and guidelines based on the) DHS upon joining the company. See control 12 related to the privacy training.<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination): | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | ▸ Standards of Business Conduct training | |
| Microsoft operates remediation methods to detect and correct personal data propagation of EUII and Customer content outside of their applicable boundaries (e.g. scans of logging for EUII). Potential incidents are documented and investigated, categorized and where applicable based on category, remediated | 5 | M | Microsoft processes all generated data in the designated boundaries, for the applicable category of personal data, i.e. EUPI, EUII, Customer Content, unless generated data is anonymized | Inquired staff and inspected the DHS, covering permissibility of data transmission, data storage and data use, and noted that<br>▸ data cannot be processed in a boundary without having been transported to that boundary<br>▸ allowable transmission between boundaries implicitly covers the processing of data in the correct boundary<br><br>Inquired staff and inspected documentation, and noted that<br>▸ the applicable DHS should always be followed<br>▸ staff privacy training is required before having access to privacy-related data<br>▸ relevant changes to software for collecting and processing of personal data requires a privacy review prior to implementation<br>▸ monitoring and follow-up is in place to verify if EUII would be leaving its boundary<br><br>Observed scrubbing of PII and PII leakage detection, and noted that these automated processes are in place. | No deficiencies noted. |
| Microsoft requires privacy incidents to be reported to Controller (i.e. in accordance with contractual and legal obligations and to enable | CTRL54 | M | Microsoft requires privacy incidents related to the user organization to be reported to user organization. | Inquired staff and inspected the Microsoft Security Standard Operating Procedures (SOP), and noted that<br>▸ Microsoft requires breaches to be disclosed to the controller without undue delay and within 72 hours, in case of breach declaration | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| Controller to inform affected users or to report to DPA) | | | | Inquired staff and inspected monthly meeting slides with regard to privacy events, and noted that<br>▸ meetings are organized monthly<br>▸ during these meetings privacy events are discussed that took place in any Microsoft environment (including development and testing environments), triggered by tooling (e.g. PII leakage detector), Microsoft staff, and Customers<br>▸ trends of privacy incidents are analyzed and monitored<br>▸ progress to resolve privacy events is monitored | |
| Microsoft processes all generated data in the designated boundaries, for the applicable category of personal data, i.e. EUPI, EUII, Customer Content, unless generated data is anonymized | 5 | M | Microsoft processes all generated data in the designated boundaries, for the applicable category of personal data, i.e. EUPI, EUII, Customer Content, unless generated data is anonymized. | Inquired staff and inspected the DHS, covering permissibility of data transmission, data storage and data use, and noted that<br>▸ data cannot be processed in a boundary without having been transported to that boundary<br>▸ allowable transmission between boundaries implicitly covers the processing of data in the correct boundary<br><br>Inquired staff and inspected documentation, and noted that<br>▸ the applicable DHS should always be followed<br>▸ staff privacy training is required before having access to privacy-related data<br>▸ relevant changes to software for collecting and processing of personal data requires a privacy review prior to implementation<br>▸ monitoring and follow-up is in place to verify if EUII would be leaving its boundary<br><br>Observed scrubbing of PII and PII leakage detection, and noted that these automated processes are in place. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | | |
| **Life cycle step:** | Disclose | | | | |
| **Profiling risk:** | ▸ Sub processor builds or uses profiles not in accordance with contract with controller, or instructions of controller<br>▸ Processor enriches profiles via enrichment by or via 3rd party | | | | |
| Audit criteria: | ▸ Sub processor only builds or uses profiles in line with instructions of Controller<br>▸ Microsoft assesses and manages profiling risks associated with 3rd parties, both at processor (Microsoft itself) and sub processor | | | | |
| Microsoft maintains its Microsoft Supplier Data Protection Requirements (DPR, designed by Microsoft procurement, CELA, and corporate security), and ensures that these are in line with Microsoft's control framework, and GDPR, including personal data and customer data handling obligations | CTRL57 | M | Microsoft maintains its Microsoft Supplier Data Protection Requirements, and ensures that these are in line with Microsoft's control framework, and GDPR, including personal data and customer data handling obligations | Inquired staff and inspected documentation, and noted that<br>▸ the Data Protection Requirements are updated at least once per year by the Supplier Security Privacy Assurance (SSPA) team<br>▸ the update includes verifying new legislation<br>▸ the Data Protection Requirements include instructions and obligations on handling personal and customer data | No deficiencies noted. |
| Microsoft maintains and communicates to Controller an accurate list of sub processors that process personal data. Changes to the list are adequately in | CTRL58 | M | Microsoft maintains and communicates to user organization an accurate list of sub processors that process personal data. Changes to the list are adequately in advance and explicitly communicated: | Inquired and inspected the Microsoft Privacy Standard, and noted that<br>▸ Microsoft requires disclosure of (changes to) the sub processors that process personal data per the contractual agreements with commercial customers<br>▸ the list of sub processors is available in the Microsoft Trust Center | Deviation noted:<br>▸ Due to the transitional situation, 14 days in advance communications |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| advance and explicitly communicated:<br>▸ 6 months in advance for EUII and Customer Content (new functions and features)<br>▸ 14 days in advance for EUPI | | | ▸ 6 months in advance for EUII and Customer Content (new functions and features)<br>▸ 14 days in advance for EUPI | ▸ the list can be added to one's library, where notifications of changes to the list can be enabled and received on occurrence<br><br>Inquired and noted that Microsoft decided per 31 July to not only disclose sub processors of EUII and Customer Content, but also EUPI.<br><br>Inspected sub processor information, and noted that a sub processor was added to the list during the audit period. This added sub processor did not concern a new sub processor, but was added as a result of the changed policies with regard to disclosing sub processors, and concerns a transitional situation. As a consequence, a 14 days in advance communications could not be provided. | was not provided<br><br>No other deviations noted. |
| In case Microsoft launches new services that have never been used by a customer, and they use a sub processor that is new to the list, then disclosure of the new sub processor occurs with the service launch, not 6 months in advance of it. Customer choice will be available with regard to the new service. | CTRL59 | M | In case a new service is launched by Microsoft that have never been used by customer and they use a sub processor that is new to the list, disclosure of the new sub processor occurs with the service launch not 6 months in advance of it. User organization's choice will be available with regard to the new service. | Interviewed staff and inspected the Microsoft Privacy Standard, and noted that<br>▸ Microsoft requires disclosure of (changes to) the sub processors that process personal data per the contractual<br>▸ the list of sub processors is available in the Microsoft Trust Center<br>▸ the list can be added to one's library, where notifications of changes to the list can be enabled<br><br>Per interview we noted that no new services were launched during the audit period. | No occurrences noted: No new services were launched during the audit period.<br><br>As a result, conditions required for the operation of the control did not occur. Therefore, we performed only design testing and no operating effectiveness testing for this control. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| Microsoft's instructs sub processors to protect personal data via its DPR, as a measure to intended to achieve suppliers' compliance to contracted clauses between Microsoft and Microsoft's customers | CTRL60 | M | Microsoft's instructs sub processors to protect personal data via its DPR. | Interviewed staff and inspected the Data Protection Requirements, and noted that<br>▸ the Data Protection Requirements include instructions and obligations for protection of personal data by sub processors, and are part of the supplier master agreement | No deficiencies noted. |
| Microsoft requires a self-attest by its sub processors yearly. Also, from time to time (e.g. based on self-attest an independent audit assessment by or on behalf of Microsoft is required, to monitor for compliance with the DPR. In all cases ISO27001, ISO27002, and ISO27018 certification is required to be maintained | CTRL61 | M | Microsoft requires self-attest by its sub processors on a yearly basis. | Interviewed staff and inspected the Supplier Security, Privacy Assurance (SSPA) program, and noted that<br>▸ sub processors must attest to comply with the Data Protection Requirements at least once per year<br>▸ this yearly attestation is included as a requirement in the supplier master agreement<br><br>Inspected the supplier information, and noted that the latest attestation of suppliers in scope was during or less than 12 months before the end of the audit period. | No deficiencies noted. |
| Microsoft assesses its suppliers, in case of suspicions of non-compliance with their obligations to Microsoft | CTRL62 | M | Microsoft assesses its suppliers, in case of suspicions of non-compliance with their obligations to Microsoft | Interviewed staff and inspected Microsoft internal communications, and noted that<br>▸ one of the sub processors was investigated based on suspicions of non-compliance<br>▸ specialized Microsoft teams decided that the sub processor was no longer compliant and blocked the use of this sub processor | No deficiencies noted. |
| When providing EUPI to sub processors, Microsoft does not provide additional identifiers or additional user or organizational | CTRL63 | M | When providing data to sub processors, only an EUPI identifier is shared. | Interviewed staff and inspected sub processor order forms to process data, from Microsoft to sub processor, and noted that | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| characteristics that would be useful for enrichment purposes, only identifier is shared. | | | | ▸ information on nature and purpose of processing, as well as types of data processed, are included in an order form<br>▸ provided data does not include customer content or EUII<br>▸ processing of data may only take place as specified in the work order for which the data was shared<br><br>Interviewed and inspected data shared with a sub processor, and noted that an identifier is shared to make analyses on the provided data possible. | |
| Microsoft provides Choice to Controller with regard to the use of optional connected services, both at tenant and user level | CTRL64 | M | Microsoft provides choice to user organization with regard to the use of optional connected services, both at tenant and user level. | Interviewed staff and inspected documentation with regard to optional connected services, and noted that<br>▸ tenant administrators can enable or disabled the use of connected services for all users in the organization<br>▸ after enabling of the connected services by tenant administrators, users can opt-in or opt-out for the use of connected services themselves, which enables or disabled these services for the user<br>▸ after disabling of the connected services by tenant administrators, the services are unavailable to all users, even when users are opted-in | No deficiencies noted. |
| **Life cycle step:**<br>**Profiling risk:**<br>Audit criteria: | Dispose<br>A data subject's profile remains available or in use, after a data subject leaves, or changes its role or function<br>▸ After disposal of user or tenant, a user's profile remains linked with the pseudonymized ID of data subject<br>▸ In case of a data subject leaving or changing its role or function, also the user's profile(s) are adjusted | | | | |
| Microsoft operates technical and organizational measures to delete personal data and | CTRL68 | M | Microsoft operates technical and organizational measures to delete personal data and | Inquired and inspected documentation, and noted that<br>▸ Instructions are available to users on how to delete files as well as (Exchange Online) mailboxes (Microsoft also | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| customer data as instructed by Controller in the diverse technical scenarios<br>▸ Upon customer instruction to delete an object (e.g. File, Email, Mailbox)<br>▸ Upon customer instruction to delete an account in the online service<br>▸ Upon customer decision to discontinue use of all the online services | | | customer data as instructed by user organization in the diverse technical scenarios:<br>▸ Upon customer instruction to delete an object (e.g. File, Email, Mailbox)<br>▸ Upon customer instruction to delete an account in the online service<br>▸ Upon customer decision to discontinue use of all the online services | has instructions on how to change the retention time of permanently deleted items for Online Exchange mailboxes<br>▸ deletion is an automated process that takes place when the instruction for deletion are given by the user organization for objects and accounts in online services. A Delete Agent processes deletion requests and tracks if deletions succeed (diagnostics data is included in the Delete Agent Health Summary)<br>▸ the retention time of deleted data is part of the DHS. In case of termination of (the subscriptions of) all online services, the customer content is retained per agreed upon commitments with the customer in the contract and in the Service Licensing Agreements<br>▸ Microsoft communicates the data retention schedule for active deletion of customer content, EUII and EUPI in the online Microsoft documentation<br><br>Inspected documentation, and noted<br>▸ instructions are present on how to delete (user) accounts within the user organization. In these instructions, it is also stated that admins have 30 days to restore the account before the user's data is permanently deleted.<br>▸ the data retention schedule for active deletion of customer content, EUII and EUPI in documented the online Microsoft documentation. This retention schedule is also part of the DHS. Admins can also force immediate permanent deletion (without the 30 days to restore) after initially deleting a user. In both cases, the admin receives a pop-up notification of successful deletion. | |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | Inquired and inspected presence of EUPI before and after deletion, and noted that deletion was performed.<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination):<br>▸ customer content within the compliance boundary is retained per agreed upon commitments with the customer in the contract and the Service Licensing Agreements | |
| Microsoft disposes of collected and generated personal data, based on its applicable data retention schedules as mentioned in the Data Handling Standard, as these personal data could be needed longer, after the requested disposal data, e.g. for the purpose of securing the services | CTRL69 | M | Microsoft disposes of collected and generated personal data, based on its applicable data retention schedules as mentioned in the Data Handling Standard, as these personal data could be needed longer, after the requested disposal data, e.g. for the purpose of securing the services. | Interviewed and inspected documentation, and noted that procedures are in place with regard to the retention period of (personal) data after deletion. The retention schedules are registered in the DHS where the least and maximum amount of days is specified per data category. For personal data (in GDPR scope), this contains the following data categories: customer content, EUII, support data, feedback data, account data, public personal data & EUPI.<br><br>Inquired and noted that a O365 customer de-provisioning and data deletion process is initiated via a signal that communicates changes to a customer's O365 subscription status. Such is a soft delete where data is retained for 25 days. After 25 days, a hard delete is initiated which causes all data to be deleted.<br><br>Note: We did not perform testing procedures for the following as these are part of SOC reporting (out-of-scope for this examination):<br>▸ deletion of customer content after the termination of the subscription | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | Inspected retention policy, and noted that the data retention schedule for active and passive deletion of customer content, EUII and EUPI in the online Microsoft documentation is communicated. This retention schedule is also part of the DHS.<br><br>Inspected documentation and noted that data handling policies and procedures address effective virtual destruction of data to protect against the possibility of data being inappropriately shared between service tenants, or being accessible after hard deletion in the service. Data deleted from the service in one tenant is not accessible to another service tenant, even if any of the underlying physical storage is reassigned.<br><br>Inspected documentation and screenshots of audit logs, and noted that synchronization requests are sent about once per minute. For a sample tenant, the organization status was changed (through multiple iterations) and that a soft delete was performed.<br><br>Inspected screenshots of audit logs after deletion, and noted that the tenant could not be found.<br>Inspected screenshot of code configuration, and noted that an organization with status 'soft delete' is hard deleted once the retention period of 25 days has passed. With this hard deletion, all data related to the organization is deleted.<br><br>Inquired and inspected presence of EUPI before and after deletion, and noted that deletion was performed. | |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| **Life cycle step:** | Data subject request | | | | |
| **Profiling risk:** | A data subject request is not timely or adequately processed | | | | |
| Audit criteria: | ▸ Legitimate data subject requests are evaluated timely and adequately for legitimacy<br>▸ Approved data subject requests are timely and adequately responded to | | | | |
| Where Microsoft processes personal data as Controller (e.g. optional connected experiences) Microsoft communicates to data subjects how to make requests associated with their data subject rights, and responds to such requests:<br>▸ In a timely manner as the GDPR requires<br>▸ Appropriately based on evaluation of the legitimacy of the request by Microsoft<br>▸ In accordance with the requirements and obligations of the GDPR | CTRL72 | M | Where Microsoft processes personal data as Controller (e.g. optional connected experiences) Microsoft communicates to data subjects how to make requests associated with their data subject rights, and responds to such requests:<br>▸ In a timely manner as the GDPR requires<br>▸ Appropriately based on evaluation of the legitimacy of the request by Microsoft<br>▸ In accordance with the requirements and obligations of the GDPR | Inquired staff and noted that<br>▸ Microsoft is only controller for optional connected services the user personally opts into<br>▸ In that scenario, the users are no longer part of the enterprise agreement, but they have entered into a direct relationship with Microsoft for the use of optional connected services<br><br>Inquired and were informed that client organization does not activate optional connected services, resulting in a non-occurrence. | No occurrences noted: optional connected services are disabled.<br><br>As a result, conditions required for the operation of the control did not occur. Therefore, we performed only design testing and no operating effectiveness testing for this control. |
| Where Microsoft processes personal data as Processor, Microsoft provide technical facilities and organizational processes together intended to enable Controller to respond to any data subject requests they may receive (consider EY audit activity, e.g. delete user, delete customer content). | CTRL73 | M | Where Microsoft processes personal data as Processor, Microsoft provide technical facilities and organizational processes together intended to enable user organization to respond to any data subject requests they may receive. | Interviewed and inspected documentation, and noted that Microsoft enables controlling user organizations to respond to any data subject requests through the 'DSR (Data Subject Request) case tool', which is part of the 'Security and Compliance' center. This tool enables the user organization to create cases for investigation, add members to the cases, find all content created by or uploaded by a specific data subject, export data and close cases once an investigation is complete. | No deficiencies noted. |

| Control activity | Control nr. | Party | Control description | Performed testing procedures | Testing Results |
|---|---|---|---|---|---|
| | | | | Observed automated DSR tooling, and noted that data subject requests are supported to be handled by the user organisation, using this tooling. | |

# Appendix 2

## 1 Complementary User Organization Controls

User organization controls as precondition for the audit. As mentioned in appendix 1, to comply with some of the criteria to mitigate risks with regard to profiling restrictions, not only Microsoft but also the user organization has to perform control activities. The relevant user organization controls are included in the table below. We have organized the User Organization Controls in line with the controls in Appendix 1 and in line with the lifecycle of data.

| Control activity | Control nr. | Party | Control description |
|---|---|---|---|
| **Life cycle step:** Notice<br>**Profiling risk:** Processor does not operate in accordance with instructions, and as a result Controller or Data subject are not aware of building or using profiles to make automated decisions<br>Audit criteria:<br>▸ Towards Controller it is transparent that profiling is in accordance with both the instructions as contracted, as well as online configuration settings<br>▸ Towards data subject, it is transparent what profiling takes place with data subject's personal data. | | | |
| Controller considers the risks and suitability of Office 365 in accordance with its own applicable criteria, i.e. determines which data can be processed by Office 365 for outcomes applicable to its circumstances | CTRL1 | UO | User organization carries out a risk analysis on a yearly basis relating to the risks and suitability of Office 365. This risk analyses contains at least an overview of data that can be processed by Office 365 and additional measures of needed. |
| Controller contracts a volume of specific SKU's (Stock Keeping Units, i.e. Microsoft Office E3 or E5), each specific SKU covers a specific set of online and offline services | CTRL2 | UO | User organization configures and monitors each tenant in line with the outcome of the risk analysis and the organizational policy. |
| Controller trains an admin to professionally manage the Office 365 tenants | CTRL3 | UO | User organization trains an admin to professionally manage the Office 365 tenants. |

| Control activity | Control nr. | Party | Control description |
|---|---|---|---|
| Controller initially instructs its service through a number of cascading levels of operable controls, including services activation per user based on contracted SKU's | CTRL4 | UO | User organization has identified operable controls and cascading levels based on the outcomes of the risk analyses. These operable controls are reviewed on a yearly basis. |
| Controller monitors service messaging (aka: notices, or via SIEM APIs) for changes to the services in use (as already instructed) and acts to issue or change their instructions to match their requirements | CTRL5 | UO | User organization monitors service messaging for changes to the services in use and acts in case changes are needed. |
| Based on changes announced or enforced by Processor, Controller configures controller operable controls to instruct the services to be delivered | CTRL6 | UO | User organization configures controls to instruct which and how services are to be delivered based on changes announced or enforced by Microsoft. |
| Controller trains their users on their permitted use of Online Services as appropriate, based on requirements to which Controller is subject (e.g., laws, regulations, workforce policies), as applicable to data processing scenarios enabled by the Online Services | CTRL7 | UO | User organization trains their users to appropriately use Online Services based on the requirements to which the user organization is subject to. |
| Controller's users provide personal data for processing (aka: "Instructions") | CTRL8 | UO | User organization's users provide personal data for processing to Microsoft, receiving awareness training with regard to privacy and use of services. |
| **Life cycle step:** | Legal Basis | | |
| **Profiling risk:** | No legal basis to profile based on instructions issued by controller | | |
| Audit criteria: | ▸ Controller allows for restricted profiling in accordance with GDPR only<br>▸ Processor performs profiling in accordance with contract and instructions only (which includes GDPR compliance) | | |

| Control activity | Control nr. | Party | Control description |
|---|---|---|---|
| Controller accepts and implements services, and maintains operable controls, to have Microsoft process personal data in line with its instructions (such includes profiling, if any) | CTRL21 | UO | User organization accepts and implements services to have Microsoft process personal data in line with instructions. |
| | CTRL22 | UO | User organization maintains operable controls to have Microsoft process personal data in line with its instructions. |
| Microsoft adequately in advance notifies Controller, if determined necessary based on trust and legal review, with regard to Microsoft's changes to existing in-production Online Service functionality, i.e. shares its actualized documentation, that is introducing processing associated with an online services feature that results in profiling, if any. Such allows Controller to apply choice with regard to new or changed functionality (consider EY audit activity covering review requests, reviews and need for documentation and notice) | CTRL25 | UO | Such allows user organization to apply choice with regard to new or changed functionality. |
| **Life cycle step:** Provide and collect<br>**Profiling risk:** Processor receives personal data un-instructed, that could be used for the purpose of profiling<br>Audit criteria: ▸ Processor only receives (provides or collects) personal data that can be used for profiling, as far as instructed | | | |
| Controller instructs its users that only allowed classes of data, i.e. personal data, are to be provided, considering its own data handling policies and guidelines, as well as its risk-based evaluation of the suitability of the Online Services | CTRL27 | UO | User organization instructs its users that only allowed classes of data, i.e. personal data, are to be provided, considering its own data handling policies and guidelines, as well as its risk-based evaluation of the suitability of the Online Services. |

| Control activity | Control nr. | Party | Control description |
|---|---|---|---|
| Controller or user instructs Microsoft, via operable controls in accordance with their requirements and legal basis, to limit the nature and extend of personal data (incl. diagnostic data) that is collected by Microsoft from software operated by Controller | CTRL28 | UO | User organization instructs Microsoft, via operable controls in accordance with their requirements and legal basis, to limit the nature and extend of personal data (incl. diagnostic data) that is collected by Microsoft from software operated by user organization. |
| **Life cycle step:** | Store | | |
| **Profiling risk:** | ▸ Personal data is accessed to build a profile without authorization<br>▸ A data subject's profile is accessed without authorization | | |
| Audit criteria: | ▸ Personal data, including profiles, are secured against unauthorized access by known and unknown users (linked to Security and Access)<br>▸ Access to personal data, including profiles, is restricted to authorized users only (refer to Security and Access) | | |
| No UO control activities identified | | | |
| **Life cycle step:** | Use and Generate | | |
| **Profiling risk:** | ▸ Processor builds or uses profiles not in accordance with contract or instructions of controller<br>▸ As a result of a new or an amended function<br>▸ As part of data analytics<br>▸ Due to privacy violation | | |
| Audit criteria: | ▸ Processor only uses profiles for the performance of the service, the security of the service and to keep the service up to date, as well as legitimate interests as far as agreed with controller, in the services' current state and as a result of changes<br>▸ Personal data, including profiles, are secured against unauthorized access by known and unknown users (refer to Security and Access)<br>▸ Access to personal data, including profiles is limited to approved users and for a limited period (refer to Security and Access) | | |
| No UO control activities identified | | | |

| Control activity | Control nr. | Party | Control description |
|---|---|---|---|
| **Life cycle step:** Disclose<br>**Profiling risk:**<br>▸ Sub processor builds or uses profiles not in accordance with contract with controller, or instructions of controller<br>▸ Processor enriches profiles via enrichment by or via 3rd party<br>Audit criteria:<br>▸ Sub processor only builds or uses profiles in line with instructions of Controller<br>▸ Microsoft assesses and manages profiling risks associated with 3rd parties, both at processor (Microsoft itself) and sub processor | | | |
| Controller subscribes to and reviews changes in the list of sub processors, to determine if these sub processors can be accepted as part of Controller's instructions. Based on the outcome of such evaluation, Controller has decision making processes to decide to remain user of the service, which includes the new sub processor, or terminate/ceases use (as applicable), or to set operable controls, if applicable | CTRL55 | UO | User organization subscribes to and reviews changes in the list of sub processors to determine if these sub processors can be accepted as part of the user organization's instructions. Based on the outcome of such evaluation, user organization has decision making processes to decide to remain user of the service, terminate/cease use or set operable controls if applicable. |
| Controller chooses with regard to the use of optional connected services, either at tenant or user level (outside of terms | CTRL56 | UO | User organizations have processes in place with regard to discussion making of the use of optional connected services, either at tenant or user level (outside of term |
| **Life cycle step:** Dispose<br>**Profiling risk:** A data subject's profile remains available or in use, after a data subject leaves, or changes its role or function<br>Audit criteria:<br>▸ After disposal of user or tenant, a user's profile remains linked with the pseudonymized ID of data subject<br>▸ In case of a data subject leaving or changing its role or function, also the user's profile(s) are adjusted | | | |

| Control activity | Control nr. | Party | Control description |
|---|---|---|---|
| Controller trains required staff with regard to Microsoft's Online Service's feature, to issue data deletion instructions to match their requirements for the diverse technical scenarios | CTRL65 | UO | User organization trains required staff with regard to Microsoft's Online Service's feature to issue data deletion instructions to match their requirements for the diverse technical scenarios. |
| Controller adequately in advance reads service change notices from Microsoft that alert to changes in the design of data deletion scenarios in the services | CTRL66 | UO | User organization has implemented a process to make sure service change notices are read and adequately followed up. |
| Controller has a process to extract or to re-assign to new named users, the customer data of deleted data subjects (users) or tenants | CTRL67 | UO | User organization has a process to extract or reassign to new named users, the customer data of deleted data subjects (users) or tenants. |
| **Life cycle step:** Data subject request<br>**Profiling risk:** A data subject request is not timely or adequately processed<br>Audit criteria: ▸ Legitimate data subject requests are evaluated timely and adequately for legitimacy ▸ Approved data subject requests are timely and adequately responded to | | | |
| Controller timely and adequately reviews legitimacy of data subject request | CTRL70 | UO | User organization has a process in place to timely and adequately reviews legitimacy of data subject request |
| Controller handles data subject's data subject request via online feature of Microsoft | CTRL71 | UO | User organization has a process in place to handle data subject's data subject request via online feature of Microsoft |