Ministry of Justice and Security

Summary of the 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

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-B/DW/ib

Samenvatting bij assurance-rapport over profiling-beperkingen bij gebruik van Microsoft's Office 365 ProPlus

Geachte heer Van den Berg,

U heeft ons gevraagd een audit uit te voeren naar de mate van dataprotectie van persoonsgegevens bij Microsoft, betreffende de wijze waarop Microsoft er voor zorgt dat profilering van persoonsgegevens wordt voorkomen. Conform ons voorstel van 4 december 2019 met kenmerk 1010034055 hebben wij deze audit uitgevoerd.

Bijgaand treft u de samenvatting aan van onze assurance-rapportage conform de NOREA Richtlijn 3000A met het kenmerk REQ5267448-A/DW/ib van 17 maart 2021. Deze samenvatting bevat zodoende dan ook niet alle informatie die in het assurance-rapportage is opgenomen, het lezen van de samenvatting kan dan ook het kennisnemen van het gehele assurance-rapportage niet vervangen.

Onze assurance-rapportage is conform uw verzoek Engelstalig opgesteld. In de bijlage ontvangt u onze Nederlandse samenvatting, met daarin de door ons uitgevoerde werkzaamheden en de belangrijkste constateringen.

Verder merken wij op dat in het kader van hoor en wederhoor onze constateringen op 18 februari 2021 met Microsoft zijn afgestemd.

Graag zijn wij 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

Introduction

This is a summary of the assurance report on profiling restrictions with regard to Microsoft's Office 365 ProPlus as agreed with the Dutch government, dated 17 March 2021. The summary does not contain all information that is included in the assurance report. Therewith, this summary does not replace the assurance report.

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.

Background

In February 2017 the Ministry of Justice and Security signed the Microsoft Business and Services Agreement ("MBSA") with Microsoft for volume licensing of various Microsoft products, including Microsoft Office 365. Additionally, in April 2017 Amendment 1 to the MBSA was agreed in view of the upcoming GDPR.

The Ministry of Justice and Security conducted various investigations about the processing of personal data in Microsoft Office 365, namely:

- Investigation by the Dutch Data Protection Authority into the processing of telemetry data when using Windows 10 Home and Pro.
- Research by the department 'Microsoft Rijk Strategic Supplier Management' of the Ministry of Justice and Security on telemetry on Windows 10 Enterprise. This is partly in view of the AVG/GDPR that has been effective since 25 May 2018.
- Research by Microsoft Rijk Strategic Supplier Management into the processing of diagnostic data when using Microsoft Office Pro Plus.
- Mid 2019, research was again done into processing of personal data by Microsoft Office 365 ProPlus, after Microsoft made improvements in its software.

As a result of these investigations, Amendment 2 to the MBSA was agreed with Microsoft Ireland Operations Ltd., to adequately mitigate the personal data protection risks of data subjects using Microsoft's Office 365 ProPlus products, including cloud services, which can now be used by The Dutch government (DPIA 11 June 2019, DPIA 22 July 2019). Also, an amendment was agreed with Microsoft Corporate, as Microsoft Corporate is the actual processor of diagnostic data.

Objective of the audit

The Ministry of Justice and Security announced to Microsoft that an audit was to be performed, concerning the prohibition of processing Customer data and Personal data for the purpose of profiling (see amendment 2 art. 3).

Based on the Ministry's request, the objective of the audit we have performed was as follows:

To provide reasonable assurance if Microsoft ensures personal data protection in Office 365 ProPlus with regard to agreed profiling restrictions, as agreed in the agreement (MBSA) and amendments between the Ministry of Justice and Security and Microsoft, during the period from 1 July 2020 to 30 September 2020.

Approach

Searching of prohibited profiling is like searching for a needle in a haystack. Therefore, EY prepared the following approach.
We considered performing data analytics procedures, to seek for prohibited profiling by Microsoft. However, considering the size and complexity of Microsoft's infrastructure performing data analytics procedures to find prohibited profiling is practically not possible.
The approach we have chosen has focused on making use of Microsoft's controls to 'prevent a needle to exist' (prohibited profiling to exist), and if 'such a needle would be detected' (prohibited profiling would be detected), an adequate response is present to 'remove the needle' (eliminate prohibited profiling).

Since Microsoft is to adhere to the contracted personal data protection requirements (agreement (MBSA) and amendments) continuously, EY assessed how Microsoft accomplishes such both in design and operating effectiveness. First, EY and Microsoft discussed the risks with regard to restricted profiling, as well as criteria that are required to mitigate these risks. Secondly, Microsoft was requested to provide its control activities (policies, procedures, and techniques, to reduce risks) that Microsoft adheres to, to manage the risk of not adhering to the contracted profiling prohibitions, and remain operationally compliant with its legal and contractual obligations regarding profiling restrictions.

The risks, criteria and control activities were structured in line with the lifecycle of the personal data, with a focus on the restricted profiling by Microsoft for Office 365 ProPlus, for:

- The Microsoft services related to delivering Office365 ProPlus for business on Windows 10 (hereafter Office 365 ProPlus)
- Collected, provided, and generated personal data related to the Office 365 ProPlus services

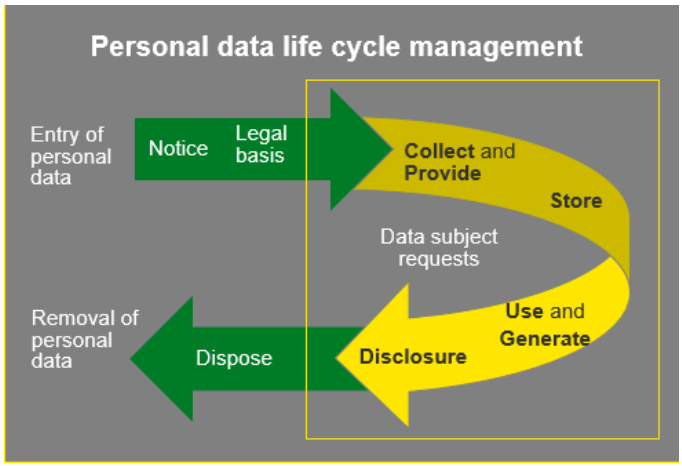

Figure – Life cycle of personal data

The risks, criteria and control activities are to 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, evaluating, and reporting of compliance
- Responding to potential non-compliances

EY validated that the criteria and control activities are designed and operated effectively to manage the risks with regard to restricted profiling of personal data.

Control activities that mitigate identified risks were assessed, as far as Microsoft is the control owner of these control activities. For this purpose, per control activity we determined the control owner, and we classified if a control activity is to be performed by Microsoft as service provider (personal data processor) or by the user organization (personal data controller). Please note that we did not audit control activities that are to be performed by the user organization. However, we did assess if identified risks would be mitigated by a combination of service provider and user organization (Ministry of Justice and Security) controls.

Results

We have examined Microsoft's controls, both their design and operating effectiveness, throughout the period from 1 July 2020 to 30 September 2020, and determined that these controls are effective to meet the control objectives, needed to ensure with a reasonable likelihood that no prohibited profiling is present with regard to Office365 ProPlus, as agreed in the agreement (MBSA) and amendments between the Ministry of Justice and Security and Microsoft.

Consequently, we consider the likelihood of prohibited profiling to be present in Office365 ProPlus as low, and if noticed, controls are in place to eliminate such prohibited profiling.

Our opinion has been formed on the basis of the matters outlined in our 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) of the assurance report.

Control objectives and controls

To audit profiling by Microsoft, the scope of the relevant audit criteria and control activities concern three areas:

- Privacy and Profiling controls
- Security and Access controls
- Entity level controls

As the Ministry of Justice and Security requested EY to focus the audit on profiling restrictions, we have focused our IT audit activities on *Privacy and Profiling* controls. In some cases we still consider *Security and Access* controls, or *Entity level* controls as relevant. In these cases we refer to these areas.

The privacy and profiling controls are structured in accordance with the life cycle of personal data (see figure). This lifecycle provides a view of personal data from the perspective of the Controller, as applying the lifecycle supports completeness of criteria and control activities.

As a Controller, the Dutch government needs to protect the personal data of individuals who make use of Office 365 ProPlus. For this purpose, as part of its outsourcing to Microsoft, the Dutch government is to instruct Microsoft, as a Processor, ensuring that the combination of Controller and Processor controls reduces the profiling risks for individuals an acceptable level.

Please note that restricted profiling implies that profiling could be allowed, e.g.:
- determine feature adoption patterns,
- feature design and availability decisions, and
- provide personalized product help about the version of the product a user is running,

to the extent consistent with the written instructions given to Microsoft and as set forth in the MBSA and Amendments.

Where Microsoft is Processor, it is the Controller's role to communicate to end-users (for which purpose Microsoft must provide the Controller appropriate information, or Controller cannot perform personal data protection requirements as they have to).

Microsoft has designed and implemented policies and guidelines (e.g. Data Handling Standard), intended to achieve that profiling is restricted, and could only be established after approval via Microsoft's methods of software development, legal reviews (incl. evaluation of necessary Notice and Choice), and with documentation and notice for the customer.

Expected user organization controls as precondition for the audit

To make use of Office 365 ProPlus, Microsoft expects that:
- User organization studies and understands current documentation for Online Service's features and acts to issue or change their instructions to match their requirements.
- User organization establishes to receive notices and communications from Microsoft and act on them appropriately.
- User organization understands that prior service activations will remain in effect until changed.

Also, the Dutch Ministry of Justice and Security expects that at tenant (user) level, as reported in the Ministry's DPIA's, the following is ensured by tenant:
- Upgrade to version 1905 or higher for Microsoft Office 365 ProPlus
- Diagnostics (telemetry) level for Microsoft Office 365 ProPlus on 'Neither'
- Telemetry level for Windows 10 Enterprise security on 'Security' or block all traffic for telemetry
- Turn Customer Experience Improvement Program (CEIP) off
- Turn LinkedIn integration off
- Do not use Office apps on mobile devices
- Disable use Controller Connected Experiences

Managing the risks with regard to profiling, as a result of the audit, we noted that a tenant (who acts in the role of Controller), making use of the contract between the Ministry of Justice and Security, and Microsoft, also is required to apply the following:

- 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.
- User organization configures and monitors each tenant in line with the outcome of the risk analysis and the organizational policy.
- User organization trains an admin to professionally manage the Office 365 tenants.
- 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.
- User organization monitors service messaging for changes to the services in use and acts in case changes are needed.
- User organization configures controls to instruct which and how services are to be delivered based on changes announced or enforced by Microsoft.
- User organization trains their users to appropriately use Online Services based on the requirements to which the user organization is subject to.
- User organization's provides awareness training with regard to privacy and use of services for processing by Microsoft.

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.