Ministerie van Justitie en Veiligheid

Information and Procurement Directorate

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
https://www.government.nl/ministries/ministry-of-justice-and-security

Contact
Paul van den Berg

M +31 6 524 704 25
E
p.j.van.den.berg@minvenj.nl

Date
17 July 2019

To whom it may concern

memo

State of Play – Microsoft

On 7 November 2018 the Strategic Vendor Management Microsoft unit (SLM Microsoft Rijk) at the Information and Procurement Department of the Ministry of Justice and Security – the central point of contact for Microsoft within central government – published an extensive report on the way in which Microsoft collects and processes personal other data through its products Office 2016 and Office 365 ProPlus. This report is known as the 'DPIA on diagnostic data in Microsoft Office ProPlus' (DPIA).

The DPIA showed that Office did not meet all the requirements of the General Data Protection Regulation (GDPR), and that Microsoft and central government needed to take several measures to align the collection and use of personal data with the requirements of the GDPR.

Prior to the publication of the DPIA, SLM Microsoft Rijk reached agreement with Microsoft on an improvement plan. In that plan, Microsoft undertook to change its products in such a way that Dutch central government would be able to use them in accordance with the GDPR. Microsoft has now made the most urgent changes in accordance with the improvement plan. These were tested by SLM Microsoft Rijk in June 2019 and found to be in order.

SLM Microsoft Rijk wanted to further restrict the collection and use of personal data and other data to prevent further extensive processing (by third parties) of personal data.

Negotiations took place with Microsoft in April and May 2019 to lay down the necessary measures in a binding agreement, provide the required legal basis and obtain adequate means of control and control rights.

Letters to parliament
Following questions from the House of Representatives, the Minister of Justice and Security, Ferdinand Grapperhaus, and the Minister of the Interior and Kingdom Relations, Kajsa Ollongren, sent two letters to parliament. The first letter, dated 20 December 2018, informed the House

about the improvement plan and the associated timetable. The second letter, dated 1 July 2019, reported on the results of the improvement plan and contained the following conclusion:

'In light of the results achieved, which have been set out above, SLM Microsoft Rijk sees no objections relating to the GDPR for organisations that fall under SLM Microsoft Rijk to use Microsoft Office ProPlus, Windows 10 Enterprise and Azure. However, organisations remain responsible in their role as data controller for deciding whether a product or service is suitable for a specific purpose. Factors such as information security and specific legalisation that applies to the organisation must also be considered.'

Conclusions
SLM Microsoft Rijk has removed the risks identified in the DPIA or has adequately mitigated them. In addition, SLM Microsoft Rijk has removed or adequately reduced comparable risks with regard to other Microsoft products and services (this applies to all services that fall under the Microsoft Online Service Terms (OSTs)), or there is sufficient prospect of removal or mitigation of such risks (this applies to other products and services, including Windows 10 Enterprise). Finally, SLM Microsoft Rijk has stipulated that it must have adequate audit rights and all agreements are binding.

Data protection impact assessments (DPIAs) can now be performed much more uniformly and efficiently by central government bodies. This approach will lead to better results and save time and money.

Limitations
It should be noted that, while the technical product changes agreed by SLM Microsoft Rijk with Microsoft have become available worldwide for all 'Enterprise' customers, this does not apply to the additional agreements in which the obligations of the data controller and the data processor are regulated. The scope of SLM Microsoft Rijk does not extend beyond central government bodies and the associated departmental and non-departmental agencies. These additional agreements therefore apply exclusively to the government bodies and non-departmental agencies that are party to the Central Government Microsoft Business and Services Agreement (MBSA) managed by SLM Microsoft Rijk. We are of course happy to help with information and advice to other parties, however.

Further limitations: Mobile Apps and Office Online
For the sake of clarity: Microsoft Office Online and the mobile Microsoft Office apps, available via the Apple Store for iOS and via Google Play for Android, have since been investigated and do not yet meet the requirements. This is explained in a second DPIA report that will be published simultaneously with the DPIAs on Windows 10 and Office 365 ProPlus. SLM Microsoft Rijk is still discussing the terms of use with

Microsoft. Using the mobile Office apps is therefore not recommended for the time being. For Office Online, it is currently not possible – despite the agreements with Microsoft – to disable Controller Connected Experiences. Therefore, using Office Online is also not recommended for the time being.

What has been achieved?

Authorised uses: purpose limitation

The DPIA identified eight risks concerning Office. The negotiations in April and May primarily concerned risk no. 6 ('lack of purpose limitations'). This risk has been removed by:

- agreeing in great detail for what purposes Microsoft may use data from the State (both content data and all data about the use of the services) that falls under the scope of the agreements between the State and Microsoft;
- prohibiting the use and transfer of data to third parties for data analytics, profiling, advertising and market research, unless this is permitted on the basis of written instructions from the State;
- agreeing in detail how data should be anonymised, in line with WP29 Opinion 05/2014 on Anonymisation Techniques (WP216);
- giving a broad scope to the purpose limitation agreements, by referring to both 'Customer Data' and personal data generated by Microsoft in connection with the use by central government of the Online Services; and
- agreeing that Controller Connected Services can be enabled and disabled centrally by administrators.

Audit

It has also been agreed that SLM Microsoft Rijk can check compliance with the agreements through audits by an independent third party appointed by SLM Microsoft Rijk. Microsoft is committed to cooperating in such audits by making the systems with which it processes data, as well as facilities and supporting documentation relevant to the processing of personal and other data of the organisations that fall under SLM Microsoft Rijk, available and giving the auditors access.

The other seven risks

As mentioned above, the negotiations in April and May 2019 focused primarily on risk no. 6. Some of the other risks had already been covered or adequately mitigated. The remaining risks were included in the April and May negotiations and were then removed or adequately mitigated.

Recording agreements and applicability to enrolments

All agreements are contained in an amendment to the highest-ranking agreement with Microsoft (the MBSA). This amendment cannot be changed at a lower level.

All additional agreements automatically apply to all enrolments that refer to the central MBSA of SLM Microsoft Rijk as of 1 May 2019, as explained in this memo. The government bodies that use the central MBSA do not have to take separate action to make the improved agreements applicable.

For the data transfers from the EU to the US that involve the use of the OST services, an appendix has been developed that meets the level of detail required by the GDPR. This appendix provides insight into which types of data are processed by Microsoft Corp. – the importer of this data – and for which Microsoft Corp. undertakes all necessary guarantees. This appendix must be completed per enrolment by the relevant government body.

SLM Microsoft Rijk will approach the government bodies that already fall under it in the coming weeks to add this appendix to the enrolment.

How to proceed with the DPIAs? - Efficiency advantage
A data protection impact assessment (DPIA) must be carried out if there are high risks to the data protection of data subjects. In a DPIA, the effects of the intended processing activities on the data protection of relevant data subjects must be assessed.

At present, all data controllers of the State (i.e. the central government bodies in this case) must each carry out their own DPIA, because they process personal data for a variety of purposes, as a result of the statutory tasks that they perform. The protection measures and contractual agreements that SLM Microsoft Rijk has agreed with Microsoft are an essential part of these DPIAs.

To prevent the data controllers from each making their own assessment of the agreements with Microsoft, SLM Microsoft Rijk has had a modified DPIA carried out for Windows 10 Enterprise and Microsoft Office ProPlus (including Office online and the mobile Office apps), on the basis of the agreements with Microsoft. This DPIA then counts as a 'technical model DPIA' that relates to Microsoft's role as a data processor and the agreement with Microsoft. All participating government bodies can then refer to this technical model DPIA when performing their DPIA. In addition to referring to the technical model DPIA, the data controllers then only have to assess their own use of the Microsoft services (i.e. the risks associated with the processing of the specific personal data that they process using the Microsoft Online Services). This benefits uniformity in risk assessment and saves a lot of time and money.

SLM advice
In summary, the advice to central government bodies is as follows:

1. Join SLM Microsoft Rijk to gain access to the required contractual conditions.
2. Use Windows 10 Enterprise (version 1903 or higher) with Timeline Sync disabled and set the telemetry to the lowest level – 'Security' – or have the telemetry traffic blocked.
3. Regarding Microsoft Office 365 products and services:
    a. Prohibit the use of Controller Connected Experiences by centrally disabling this function.
    b. Use version 1905 or higher of Office 365 ProPlus and set the telemetry level to 'Neither'.
    c. Disable the sending of data for the Customer Experience Improvement Program.
    d. Disable the LinkedIn integration with Microsoft employee work accounts.
    e. No DPIA has been carried out for Workplace Analytics and Activity Reports in the Microsoft 365 admin center. There is also no DPIA for user access to MyAnalytics and Delve. If organisations want to use these tools, they must perform a DPIA. To this end, they can contact SLM Microsoft Rijk.
4. Depending on the specific situation in each organisation, the use of Customer Lockbox and Customer Key can be considered, as a way of further protecting the content of files.
5. Do not use Office Online and the mobile Office apps that are part of the Office 365 licence until the five high risks described in the DPIA addendum have been mitigated.

Documentation
A considerable amount of documentation, including the DPIAs and an implementation guide, has been published on government.nl.

Paul van den Berg
Strategic Vendor Manager, SLM Microsoft Rijk