Ministry of Justice and Security

UNCLASSIFIED
CIO Board
Ministry of Justice and Security CIO Council
Ministry of Justice and Security CTO Consultation Committee

Information and Procurement Directorate
Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.government.nl
Contact
Paul van den Berg
p.j.van.den.berg@minvenj.nl
T +31 (0)6 5247 0425

Advice on Windows 10 Enterprise and Office 365 Telemetry

Date
11 February 2018

Project name
SVM Microsoft

Our reference
2205531

Annexes
0

Cc

AVG@VenJ
Microsoft

Advice from Strategic Vendor Management Microsoft to central government organisations

The contract between Microsoft and central government was concluded in August 2017. The MBSA amendment to that contract, which includes requirements for online services, states that the Ministry of Justice and Security (representing central government) and Microsoft jointly agree that Microsoft will use information gathered from customers (i.e. staff working for central government, the police and relevant non-departmental agencies) only to provide contracted online services. Other use is not permitted. As this telemetry data is not gathered by the contractor, Microsoft Operations Ireland, but by Microsoft Corporation USA (which must be designated as the [i]data controller for this data), the MBSA amendment must first be expanded, if the use of Windows 10 Enterprise with the recommended telemetry settings is to comply with the General Data Protection Regulation (GDPR).

In order to ensure that organisations purchasing and using Windows 10 meet all the requirements set by the regulation, SVM Microsoft advises the following action:

1. Postpone the rollout of Windows 10 Enterprise until the conditions below have been met:
   a. The intended version of Windows 10 Enterprise (Redstone 4) is available for use (general availability release: April 2018).
   b. The security settings have been tested and are available and/or the script to disable telemetry is available and has been checked on behalf of the organisations opting to use this script.
   c. SVM Microsoft, in cooperation with several ministries, has carried out a data protection impact assessment (DPIA) of Windows 10 Enterprise and Office 365. The results will be shared with all central government organisations, so that their data protection officers can each decide.

   d. Microsoft has made available all the information required to carry out the DPIA.
   e. SVM Microsoft has made additional contractual arrangements concerning the responsibilities of joint controllers, as described in article 26 (1) of the General Data Protection Regulation.

2. In the short term, until the situation surrounding telemetry within Windows 10 and Office 365 is fully clear, conclude no contracts apart from **SA only** or (for rented software) **on-premises** contracts, since it is not possible to choose an Office 365 package that complies with the General Data Protection Regulation.

Background

On 10 January 2018 a meeting was held between SVM Microsoft (the Ministry of Justice and Security) and various central government organisations (including the police and non-departmental agencies) regarding the SML Microsoft Rijk annual plan for 2018. One of the main agenda points was a presentation and Q&A session by the Data Protection Authority's senior researcher, who is responsible for matters concerning Microsoft.

During the meeting, the Data Protection Authority's recently published report on the gathering and transmitting of users' personal data by Microsoft via Windows 10 Home and Pro was explained and discussed. The Data Protection Authority's conclusion is that, as far as Windows 10 Home and Pro are concerned, Microsoft is in breach of section 6 of the Personal Data Protection Act (WBP) (article 5 of the General Data Protection Regulation) and section 8 of the Personal Data Protection Act (article 6 of the General Data Protection Regulation).

The corporate and public sectors generally use another version of Windows 10: Windows 10 Enterprise. The Data Protection Authority has not examined this version. Windows 10 Enterprise has been examined – to a limited extent – by the Bavarian Data Protection Authority. Their findings show that users' personal data is collected in Windows 10 Enterprise too, but that this feature can be disabled. This cannot be done by users themselves, but rather through action taken by administrators.

The Dutch Data Protection Authority has not examined Windows 10 Home or Pro in combination with Microsoft Office 2016 and Office 365. Microsoft itself has now confirmed that Office 2016 and Office 365 also have data collection features. As yet, very little is known in this regard and no one has yet looked into the issue. So far, Microsoft has not provided any information on whether other services/products also collect personal data.

Outcomes of meetings with Microsoft

Last month, a delegation from the Ministry of Justice and Security – given its role as SVM Microsoft – visited Microsoft HQ in Seattle in order to discuss a range of issues with Microsoft's management, including the situation that has arisen.

Information and Procurement Directorate

Date
11 February 2018

Our ref.
2205531

The Windows Technology Product Group's legal team informed the delegation that they were informed of the Data Protection Authority's view that some Microsoft products fail to comply with the EU's General Data Protection Regulation. The team also stated that they are aware that the EU's ePrivacy Regulation may mean that Microsoft products must meet additional requirements.

During the visit, Microsoft delivered several PowerPoint presentations highlighting the improvements contained in the next Windows update, which has the working name ‘Redstone 4’. They expect that these improvements will make the products in question compliant. The new version of Windows is expected to go on general release in April 2018. The delegation noted that these undertakings were given only by the Windows Technology Product Group – not by other product groups (e.g. the Office Product Group).

The Windows Technology Product Group highlighted the following improvements:

1. Microsoft will provide an OFF feature for telemetry (by way of an administrator script called ‘ZeroEmissions’). This script will turn off all dataflows from Windows 10 to Microsoft. However, there are various drawbacks in deactivating telemetry. One of them is that the desired security features – which are needed for malware detection and threat analysis – will also be deactivated. This makes the Windows products less effective and additional third-party software products will be required to ensure optimum security. Apart from the fact that using the ZeroEmissions script will devalue the Microsoft technology that has been purchased, it will also significantly increase management costs and impede future innovation. Microsoft's advice is therefore to not turn off telemetry altogether, but to set it to ‘Basic', and use a number of other data elements that are required for the security-related features.

2. Microsoft will add a button to Windows Enterprise that, once a user activates it, will immediately delete all telemetry data stored by Microsoft in the US. Users must periodically activate this button.

3. The data gathered by Windows 10 will be made visible on each PC through a JSON file that can be used in combination with a dataviewer tool.

4. Windows 10 security and privacy settings are being redesigned. Although the number of settings will increase, they will be clearer and more user-friendly.

5. In due course, it will become possible to centrally review the JSON files stored on all of the organisation's PCs.

Unresolved points

Information and Procurement Directorate

Date
11 February 2018

Our ref.
2205531

To meet all the requirements set out in the General Data Protection Regulation, organisations that purchase and use Microsoft products must take a closer look at a number of issues. Information from and cooperation with Microsoft are needed for this, and several points have still not been fully resolved or investigated, even following the delegation's visit to Microsoft HQ. They are as follows:

1. Microsoft agrees with the Data Protection Authority that Microsoft has the role of 'data controller' as far as telemetry is concerned. After all, it is Microsoft that determines which data is gathered from each PC and user, as well as the data's format and why, when, how and how often this data is sent to Microsoft Corporation in the US. But, in the case of an employer who provides employees with a PC running Windows 10 (with or without Office), a 'joint controllers' situation arises, as referred to in article 26 of the General Data Protection Regulation. However, the Microsoft legal team that met with the delegation believe no additional contracts are needed in order to regulate the joint controller roles of Microsoft and central government. SVM Microsoft, on the other hand, believes article 26 (1) of the General Data Protection Regulation specifies that there must be clear agreements on paper, and that article 26 (2) specifies that these agreements must be made available to the data subjects (in this case, the users).

2. It is still unclear whether the ZeroEmissions script will also stop telemetry with regard to optional software like Office 365. It is also unclear what the impact on Office 365 will be if telemetry is disabled. The Windows Technology Product Group legal team has made it known, however, that the ATA (advanced threat analytics) feature will no longer work.

The exact details regarding the use of telemetry in Office 365 have, as yet, not been made known to SVM Microsoft.

Action plan (until 30 April 2018)

1. SVM Microsoft will monitor in detail the prerequisites mentioned above and will distribute an update on the situation every two weeks.
2. New information and documents will be published in the central government collaborative workspaces. Staff members can register by email to receive updates.
3. SVM Microsoft is responsible for coordinating the DPIA. Additional outside experts will be brought in to assist with this. An interministerial working group will provide oversight.
4. A second working group (yet to be established) will negotiate the contractual and legal aspects with Microsoft. This working group will be created by the end of February 2018, under the supervision of SVM Microsoft.
5. Since steps need to be taken to check whether the measures to limit telemetry work, SVM will help set up a test lab, where telemetry can be looked at in more detail and checks can be carried out to see whether personal data is being sent to Microsoft and, if so, what data is being sent.

Conclusion

We are aware that the information and recommendations contained in this memorandum could have a significant impact on workstation projects throughout central government. We wish to stress that SVM Microsoft only provides general advice. Whether the advice has consequences for actual projects (and, if so, what these consequences are) must be determined by the individual organisations themselves.

Compliance with applicable legislation (including the General Data Protection Regulation and the ePrivacy Regulation) is not optional, however. We wish to highlight the fact that postponing further implementation/rollout or continuing to work with an on-premises solution (which is compliant or can be made to be so) will cost significantly less money in the long run than prematurely selecting a product that later proves impossible to make compliant and subsequently rectifying the situation.

We are aware that this memorandum will no doubt lead to many additional questions. The SVM Microsoft team can help central government organisations develop a strategy that works for them.

[i] This document has been translated from the original Dutch version. Some minor changes have been made to improve readability in English and individual's names have been removed