DTIA Microsoft Teams, OneDrive and SharePoint Online

If an organisation wants to use a cloud service, and personal data are transferred outside of Europe/EEA to countries without an adequate data protection level, the risks of undue access to such data must be mapped. For example, if law enforcement authorities or security services demand access, or intercept the personal data relating to European users. Such a risk assessment is called a Data Transfer Impact Assessment (DTIA).

Strategic Vendor Management Microsoft, Google and AWS for the central Dutch government (SLM Rijk) has performed a DTIA for Microsoft transfers of personal data from its Dutch government customers to the United States of America (USA). This DTIA accompanies the Data Protection Impact Assessment on Microsoft Teams, OneDrive and SharePoint Online, published 21 February 2022.

Legal analysis

The DTIA is based on the findings of the Schrems-II judgement of the Court of Justice of the European Union, Schrems-II[1] which invalidated the EU-US Privacy Shield. In addition, the detailed guidance from the European Data Protection Board (EDPB) was studied extensively.[2]

In the DTIA the risks are mapped for the 7 relevant use cases: Streaming Content Teams, Stored Content OneDrive and SharePoint, Diagnostic Data Telemetry, Diagnostic Data Service logs, Support Data Teams, OneDrive & SharePoint, Security incidents and Account Data Teams, OneDrive & SharePoint. For this DTIA (in Excel) a format was used drafted by mr. D. Rosenthal, as distributed to IAPP members, and shared under Creative Commons license. Privacy Company has tweaked the format, and has added a specific risk analysis for data subjects. Moreover, SLM Rijk has commissioned international Law firm Greenberg Traurig LLP to conduct an extensive legal analysis based on the step 3 of the Recommendations concerning the international transfers from the EU/EEA to the USA. This legal analysis is shaped in the form of a Q&A and published together with the DTIA for further use in the Dutch public sector.

Outcome

The most important outcome of the DTIA is that it is extremely unlikely that personal data from Dutch government customers are unlawfully accessed by US authorities, or by authorities in other countries where Microsoft uses subprocessors. Microsoft has publicly stated that it has never disclosed any personal data from any EU public sector customer to any government, including US authorities and services. The default encryption of all traffic in transit from the EU to the USA prevents interception of the data in the clear, and has shifted the focus from bulk surveillance to targeted interception. Last but not least, Microsoft will keep almost all personal data processing from its EU customers within the EU by the end of 2022 (with the exception of some Security Data). This is called the EU Data Boundary.

[1] Judgment ECJ-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems.
[2] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protections on personal data v.2.0.

The DTIA concludes that there are no high transfer risks when Microsoft's cloud services are used for regular communications and file storage, as long as it doesn't involve sensitive personal data. If Dutch government organisations follow the recommended measures, the transfer of regular personal data and pseudonymous Diagnostic Data through Teams, OneDrive and SharePoint Online is permitted.

The DTIA does identify two potential high risks when Microsoft Teams is used to share special categories of personal data (such as health data, or data about sexual or political orientation). Even though Microsoft processes such Customer Content Data of its EU customers in its data centres in the EU, the data are theoretically accessible to Microsoft in plain text. Microsoft does not yet offer end-to-end-encryption (E2EE) for Teams conversations with more than 2 people, and such encryption is technically not possible for cloud recordings of Teams conversations. When Microsoft itself applies the encryption, Microsoft can also remove the encryption when it is ordered to disclose these data by US judges or secret services. The actual chance that this risk occurs is extremely low. However, in view of the extremely high impact of the possible disclosure of special categories of data, the transfer risk for data subjects is nonetheless assessed as high, in line with the EDPB guidance.

Risk Mitigation

The DTIA is part of the umbrella DPIA on Microsoft Teams, OneDrive SharePoint Online and Azure AD, published by SLM Rijk on 21t February 2022.[3] The DPIA provides a table of risk mitigating measures for the identified risks.

The two most important measures for Dutch government organisations and universities are:

- Do not exchange special categories of personal data via Teams calls that are not end-to-end encrypted,
- Apply a self-controlled key whenever possible (in unscheduled 1-on-1 calls in Teams, and *Double Key Encryption* for files with special categories of data stored in OneDrive).

The two most important measures for Microsoft are:

- Commit to a clear deadline when E2EE will be supported for Teams group meetings and chat.
- Complete the EU Data Boundary as soon as possible.

Caveat

SLM Rijk has based the Data Transfer Impact Assessment on a wide range of sources. However, the development of transatlantic relations between the EU and the US is primarily a political topic, not an issue that can be solved with a legal analysis. SLM Rijk will continue to closely monitor all developments and guidance from the national supervisory authorities, and update this DTIA whenever that becomes necessary.

[3] The full report can be downloaded here