Datenschutz beim Microsoft-Produkt Teams

Die Probleme beginnen bereits damit, dass Microsoft nicht transparent arbeitet und Informationen erst nach schwierigen und umständlichen Nachfragen heraus gibt. Dies gilt insbesondere, wenn es um die so genannten Telemetriedaten geht. Microsoft sammelt diese Daten, um Informationen zur Diagnose und Metadatenauswertung zu bekommen. Auch enthalten diese Daten Informationen über die Nutzung und die Leistung von Anwendungskomponenten. Diese Inforationen können über eine ID dem Nutzer zugeordnet werden. Allerdings können Nutzer in den Programmeinstellungen die Verarbeitung ihrer Diagnosedaten reduzieren. Man muss allerdings wissen, wie dies möglich ist. Die niederländische Regierung, welche die Datenschutzkonformität von Microsoft 365 (ehemals Office 365), zu dem Teams gehört, prüfen ließ, bezweifelt, dass für die Verarbeitung der Telemetrie- und Diagnosedaten überhaupt ein Personenbezug notwendig ist.

Nutzt Microsoft die Telemetrie- und Diagnosedaten für die Produktentwicklung und die Unterstützung von maschinellem Lernen, ist dies keine weisungsgebundene Tätigkeit im Sinne des Art. 28 DSGVO. Dies ist in den so genannten OST(Online Services Teams)- Vertragsbedingungen für die Nutzung von Microsoft 365 geregelt, die Microsoft jederzeit und einseitig ändern kann. Das kann Nachteilig für den Nutzer sein.

Da Microsoft die Telemetrie- und Diagnosedaten für mindestens 30 Tage und maximal bis 18 Monate auf Servern in den USA speichert, ist ein zugriff für Produktentwicklung und Analysezwecke in dieser Zeit möglich. Im Einzelfall kann ein Microsoft-Team Teile dieser Daten auch länger nutzen.

Aus diesen im ersten Blick dürren Analysen ergeben sich aber durchaus Datenschutzrisiken.

- Nutzer können nicht wirklich abschätzen, welche Datenschutzrisiken aufgrund der fehlenden Transparenz mit der Verwendung von Microsoft 365, und damit auch von Teams, für sie verbunden sind.
- Dass sich Microsoft allein als Auftragsverarbeiter versteht, ist datenschutzrechtlich bedenklich. Die Gestaltung in gemeinsamer Verantwortung gem. Art. 26 DSGVO wäre hier Datenschutzkonformer.
- Ungeklärt ist die Zweckbindungspflicht. Während Art. 5 Abs. 1b der DSGVO fordert, dass der Zweck der Datenverarbeitung vor der Erhebung festgelegt wird, lässt die Microsoft bei den Telemetrie- und Diagnosedaten im Allgemeinen.
- Dass die Telemetrie- und Diagnosedaten außerhalb des Geltungsbereichs der DSGVO übermittelt werden ist zur Zeit aufgrund des bestehenden EU-US Privacy Shields rechtens. Doch dessen Wirksamkeit etc. wird derzeit vor dem EuGH überprüft.
- Völlig ungeklärt ist noch, wie sich Microsoft im Falle einer Herausgabeforderung von US-Behörden (z.B. der NSA) verhält. Der CLOUD-Act (Clarifying Lawful Overseas Use of Data Act) verpflichtet US-Firmen zur Herausgabe von bei ihnen gespeicherten Daten von Nicht-US-Bürgern. Nach US-amerikanischer Rechtsauffassung ist dies auch ohne ein Rechtshilfeersuchen an die zuständigen europäischen Sicherheitsbehörden möglich.
- Das europäische Datenschutzrecht schreibt vor, dass Daten zu löschen sind, wenn ihr Zweck erfüllt wurde oder eine gesetzliche Aufbewahrungszeit abgelaufen ist. Die Aufbewahrungsdauer der Diagnosedaten verstößt deshalb gegen die Löschpflicht aus Art. 17 Abs.1 der DSGVO.

Mit erhöhtem Datenschutzrisiko ist auch die Nutzung der Web-Version von Microsoft 365 verbunden, da die Cloud-Dienste von OneDrive womöglich auch nicht sicher sind. Auf die Speicherung von vertraulichen Informationen dort sollte verzichtet werden.

Bei der Nutzung von Controller Connect Experiences (z.B. den Übersetzungsdiensten) sammelt Microsoft Nutzungsdaten in einem nicht bekannten Umfang.

Auch wenn Microsoft seine Datenschutzeinstellungen ständig anpasst, ist die Nutzung seiner Dienste (inclusive Teams) nur unter den Bedingungen möglich, die Microsoft wie folgt beschreibt:

„Anstatt als statisches Software-Programm auf Ihrem Gerät installiert, basieren die Schlüsselkomponenten von Windows auf Cloud und beide, sowohl Cloud als auch lokale Elemente von Windows werden regelmäßig aktualisiert, um Ihnen die neuesten Verbesserungen und Features zu bieten. Um dieses Computer-Erlebnis anzubieten, erheben wir Daten über Sie, Ihr Gerät und wie Sie Windows verwenden.“

https://privacy.microsoft.com/de-DE/privacystatement#mainnoticetoendusersmodule

Aus den veröffentlichen Dokumenten der Berliner Datenschutzbehörde wird deutlich, dass sie Dienstleitungen von Microsoft, namentlich Teams und Skype, sowie die Videokonferenzlösung von Zoom (letztes mit Stand vom 02.04.2020) für nicht datenschutzgerecht hält. Dies stellt die Behörde in ihrer veröffentlichten Checkliste noch einmal ausdrücklich klar. Dort heißt es:

„Wir weisen darauf hin, dass einige verbreitet eingesetzte Anbieter die aufgeführten Bedingungen nicht erfüllen, darunter Microsoft, Skype Communications und Zoom Video Communications.“

Ergänzung: der stets lesenswerte Kuketz-Blog hat das hier auch ausführlich dargelegt.