Handreichung

Nutzung von Microsoft-Produkten durch EU-Institutionen

Ergebnisse der Untersuchung des Europäischen Datenschutzbeauftragten zur Nutzung von Microsoft-Produkten durch EU-Institutionen

Stand: 17. Juli 2020

VITAKO
Bundes-Arbeitsgemeinschaft der
Kommunalen IT-Dienstleister e.V.

Ergebnisse der Untersuchung des Europäischen Datenschutzbeauftragten zur Nutzung von Microsoft-Produkten durch EU-Institutionen

Link zum Dokument (Engl.)

Kontext: Die EU-Kommission hat bereits einen Zusatzvertrag mit Microsoft geschlossen, der den Empfehlungen des Europäischen Datenschutzbeauftragten (EDPS) folgt und den EU-Institutionen den Einsatz von Microsoft-Produkten ermöglicht.

Der Fokus der Untersuchung liegt auf dem Inter-Institutional Licensing Agreement (ILA), welches 2018 zwischen den EU-Institutionen und Microsoft geschlossen wurde. Die Bedingungen des ILA sind nicht eindeutig festgelegt, da Microsoft regelmäßig referenzierte Bestandteile wie z. B. die Online Service Terms (OST) ändert. Welche Version jeweils gilt, kann vom Zeitpunkt des Produktkaufs, der Verlängerung eines Abonnements oder in Teilen auch vom Erscheinen neuer Features abhängen.

Ergebnisse und Empfehlungen

- Microsoft agiert intransparent als Verantwortlicher (Art. 4 1. DSGVO). Dies basiert auf folgenden Aspekten des ILA:
    - Microsoft hat das unbegrenzte Recht, referenzierte Bestandteile wie die OST einseitig zu ändern. Hinzu kommt, dass die Rangfolge der einzelnen Dokumente unklar bleibt.
    - Die Datenschutzpflichten von Microsoft sind begrenzt auf spezifische Arten der Verarbeitung und Kategorien von Daten. Andere Datenverarbeitungen fallen nicht unter diese Datenschutzpflichten, dies trifft auch auf „Diagnostikdaten“ aus Windows und Office-Produkten zu. Es besteht das hohe Risiko, dass Microsoft als Verantwortlicher für alle Daten, die im Rahmen des ILA verarbeitet werden, agiert.
    - Die Datenverarbeitungszwecke (Art. 5 (1) b) DSGVO) sind unzureichend begrenzt. Welche Zwecke im Rahmen des ILA erlaubt sind, kann weit ausgelegt werden.

Empfehlungen: EU-Institutionen sollten als alleinige Verantwortliche festgeschrieben werden. Die Rangfolge der Vertragsdokumente sollte festgelegt werden und Änderungen an diesen dürfen nur gemeinsam vorgenommen werden. Datenkategorien und Verarbeitungszwecke sollten präzise festgelegt werden. All diese Änderungen sollten im höchstrangigen Dokument geregelt sein.

- Viele der laut DSGVO zwischen Verantwortlichem und Auftragsverarbeiter (Art. 4 8. DSGVO) festzulegenden Aspekte sind im ILA nicht klar geregelt.
  Empfehlung: EU-Institutionen sollten mit Microsoft einen umfassenden Auftragsverarbeitungsvertrag (Art. 28 (3) DSGVO) schließen.

- Das ILA ermöglicht EU-Institutionen nicht die Kontrolle über Unterauftragsverarbeiter (Art. 28 (2) DSGVO), da Microsoft für einige Datenkategorien eine Generalerlaubnis gegeben wird, diese zu beauftragen und für viele andere Datenkategorien überhaupt keine Regelung existiert. Die Informationen, die Microsoft zu den Unterauftragsverarbeitern bereitstellt, sind nicht ausreichend.
  Empfehlungen: Im ILA sollte festgeschrieben werden, dass Microsoft umfangreiche Informationen zu Datenschutz- und Sicherheitsmaßnahmen der Unterauftragsverarbeiter bei seinen einzelnen Produkten und Diensten bereitstellt, jede Beauftragung von Unterauftragsverarbeitern schriftlich zu autorisieren ist und den EU-Institutionen vorbehalten ist, einzelne Unterauftragsverarbeiter abzulehnen ohne Einschränkungen bei Diensten hinnehmen zu müssen.

- Das ILA erlaubt den EU-Institutionen nicht in ausreichendem Maße, die Einhaltung der Datenschutzverpflichtungen durch Microsoft und Unterauftragsverarbeitern zu auditieren. Die Bestimmungen hierzu bleiben zu unspezifisch.
  Empfehlung: Das ILA sollte den EU-Institutionen detaillierte Auditierungsrechte gewähren und Microsoft verpflichten, alle relevanten Informationen bereitzustellen.

- Laut den OST speichert Microsoft nur einen Teil der Daten in der EU. Die EU-Institutionen können nicht prüfen, wohin und auf welche Weise Daten außerhalb der EU

transferiert werden. Personenbezogene Daten dürfen nach Art. 48 DSGVO nur auf Anfragen von Drittstaaten herausgegeben werden, wenn ein entsprechendes internationales Abkommen mit der EU existiert. Die Datenschutzerklärung von Microsoft erlaubt dagegen die Herausgabe, wenn Microsoft sich dazu gesetzlich verpflichtet sieht, ggf. auch ohne Betroffene, zu informieren. Datenverantwortliche müssen aber den Schutz der Daten im Drittland als auch beim Transport sicherstellen.
Empfehlungen: Das ILA sollte für jedes Produkt oder jeden Service festlegen, wo Daten gespeichert und verarbeitet werden und Microsoft muss verpflichtet werden, Schutzmaßnahmen für den Transport zu ergreifen. Microsoft darf Daten nicht an Drittstaaten herausgeben und muss die EU-Institutionen über solche Anfragen informieren. Grundsätzlich sollten personenbezogene Daten, die durch Microsoft oder Unterauftragsverarbeiter verarbeitet werden, in der EU bleiben.

- Windows und Office übermitteln Diagnostikdaten an Microsoft.
  Empfehlung: EU-Institutionen sollten die Datenflüsse aus Microsoft-Produkten überwachen und sich über technische Maßnahmen zum Stoppen unerlaubter Datenübertragungen austauschen.

- Die unklaren Vertragsstrukturen machen es den EU-Institutionen schwer, ihren Informationspflichten gegenüber betroffenen Personen nachzukommen.
  Empfehlung: Es muss hinreichende Klarheit über die Speicherung und Verarbeitung personenbezogener Daten erlangt werden, um Betroffene transparent informieren zu können.

- Schlussfolgerungen: Der EDPS rät davon ab, Auftragsverarbeiter zu engagieren, die nicht willens sind, ausreichende Garantien zu geben, dass die Anforderungen der DSGVO eingehalten und die Daten von Betroffenen geschützt werden. Um dem Prinzip des Datenschutzes „by design“ nachzukommen, sollte immer geprüft werden, ob datenschutzfreundlichere Software-Alternativen verfügbar sind. Der EDPS erkennt an, dass die gegebenen Empfehlungen für viele Organisationen eine große Herausforderung darstellen, es scheint jedoch möglich den Datenschutz zu verbessern, wenn

Anbieter bereit sind, auf die Compliance-Anforderungen der Kunden einzugehen. Daher sollten Verantwortliche sich von Verhandlungen nicht entmutigen lassen, selbst gegenüber schwergewichtigen Konzernen.

Position Vitako:

Die Untersuchung des Europäischen Datenschutzbeauftragten bezieht sich auf die EU-Institutionen, jedoch ist anzunehmen, dass auch die Verträge anderer öffentlicher Institutionen mit Microsoft (oder anderen großen Software-Konzernen) ähnliche kritische Punkte enthalten. Vitako empfiehlt daher dringend, dass dort, wo solche Verträge bestehen, diese durch die zuständigen Datenschutzbeauftragten auf die in der Untersuchung aufgezeigten Probleme geprüft werden. Sollten dabei ähnliche Schwachpunkte bezüglich des Datenschutzes gefunden werden, müssen diese möglichst beseitig werden. Bis Anpassungen an den Verträgen umgesetzt werden können, empfiehlt Vitako möglichst den Einsatz von datenschutzfreundlichen Software-Alternativen, mindestens aber Maßnahmen zur Minderung der Datenschutzrisiken. Dazu verweist Vitako auch auf seinen Handreichung Zur Nutzung von Office-Anwendungen.

*Hinweis zum EuGH-Urteil vom 16.07.2020 in der Rechtssache C-311/18:

Die Ergebnisse der Untersuchung des EDPS sind hiervon nicht direkt betroffen, da zwar der Privacy-Shield-Beschluss 2016/1250 für ungültig erklärt wird, aber nicht der Beschluss über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern. Der EuGH unterstreicht dabei nochmals, dass Verantwortliche und Auftragsverarbeiter prüfen müssen, ob die Standardvertragsklauseln in einem Drittland eingehalten werden. Auch die Datenschutzaufsichtsbehörden werden verpflichtet, dies zu beurteilen. Sofern Verträge, wie oben empfohlen geprüft werden, ist also dringend darauf zu achten, dass auch die datenschutzrechtlichen Anforderungen der Standardvertragsklauseln erfüllt werden.