Handreichung

Aktuelle Entwicklungen im Bereich Datenschutz

Untersuchung des Europäischen Datenschutzbeauftragten zur Nutzung von Microsoft-Produkten durch EU-Institutionen und Urteil des Europäischen Gerichtshofs zum Privacy Shield („Schrems II“)

Stand: 1. September 2020

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

Mehrere Dokumente von der europäischen Ebene haben wichtige Auswirkungen auf die Bereiche digitale Souveränität und Datenschutz. Der Europäische Datenschutzbeauftragte hat bei einer Untersuchung der Verträge der EU-Institutionen mit Microsoft erhebliche datenschutzrechtliche Mängel festgestellt und gibt Empfehlungen, wie diese zu beheben sind. Ähnliche Schwachstellen könnten auch in den Verträgen anderer öffentlicher Institutionen zu finden sein. Daher fasst der erste Teil die Ergebnisse der Untersuchung zusammen.

Der Europäische Gerichtshof hat mit seinem Urteil in der Rechtssache C-311/18 („Schrems II“) das Privacy-Shield-Abkommen zwischen der EU und den USA für ungültig erklärt. Damit ist der Übertragung von personenbezogenen Daten in die Vereinigten Staaten in vielen Fällen die Rechtsgrundlage entzogen. Der zweite Teil erläutert die Auswirkungen und welche Optionen nun bestehen.

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 des EDPS

- 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 über-

wachen 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.

Vitako-Empfehlungen:

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.

Urteil des Europäischen Gerichtshofs zum Privacy Shield („Schrems II“)

Auswirkungen des Urteils

Am 16.07.2020 hat der Europäische Gerichtshof (EuGH) sein Urteil in der Rechtssache C-311/18 („Schrems II“) gesprochen und damit das Privacy-Shield-Abkommen zwischen der EU und den USA aufgrund der Rechtslage in den Vereinigten Staaten für ungültig erklärt. Datenschutzrechtlich ergeben sich daraus massive Konsequenzen. Alle Übertragungen von personenbezogenen Daten aus Europa in die USA, die auf Basis des Privacy Shields stattfanden, hatten mit unverzüglicher Wirkung keine Rechtsgrundlage mehr. Die Standardvertragsklauseln können zwar weiterhin genutzt werden, sind aber allein für eine Datenübertragung in die USA nicht ausreichend, da der EuGH die Verantwortlichen (Art. 4 7. DSGVO) und die Datenschutzbehörden in die Pflicht nimmt, zu prüfen, ob in dem entsprechenden Drittland ein mit dem europäischen vergleichbares Datenschutzniveau sichergestellt ist, und ggf. „zusätzliche Maßnahmen“ zu ergreifen, um den Schutz der Daten abzusichern. Die Begründung für die Ungültigkeit des Privacy Shield macht dabei deutlich, dass der EuGH den Datenschutz in den USA aufgrund der weitreichenden Zugriffsrechte der Geheimdienste nicht als ausreichend ansieht.

Dies betrifft auch digitale Dienste, wie Videokonferenzen, Cloud-Dienste und andere Anwendungen, von US-Anbietern, bei denen Nutzerdaten in die USA übertragen werden. Die Auftragsverarbeitungsverträge (Art. 28 (3) a) DSGVO), die Kommunen oder IT-Dienstleister mit diesen Dienstanbietern geschlossen haben, sind in den meisten Fällen nicht mehr ausreichend.

Welche Möglichkeiten der Datenübertragung bestehen noch?

Der Europäische Datenschutzausschuss (EDSA) oder z. B. der Landesdatenschutzbeauftragte (LfDI) des Landes Baden-Württemberg versuchen Hilfestellungen zu geben, wie Verwaltungen

und Unternehmen Datenübertragungen nun rechtssicher gestalten können. Eine Möglichkeit besteht in der Nutzung der Standardvertragsklauseln als Rechtsgrundlage mit der Absicherung durch zusätzliche Maßnahmen. Diese könnten darin bestehen, Daten nur verschlüsselt zu übertragen, wobei nur der Verantwortliche (Art. 4. 7. DSGVO) die Schlüssel besitzt, der Auftragsverarbeiter (Art. 4. 8. DSGVO) aber keinen Zugriff hat. Eine zweite Option wäre die Anonymisierung oder Pseudonymisierung der Daten vor der Übertragung, sodass nur der Verantwortliche (Art. 4. 7. DSGVO) eine Zuordnung zu den betroffenen Personen vornehmen kann.

Zusätzlich schlägt der baden-württembergische LfDI einige Änderungen und Ergänzungen der Standardvertragsklauseln vor. Solche Maßnahmen mit marktmächtigen US-amerikanischen Dienstanbietern auszuhandeln, dürfte für einzelne Behörden oder IT-Dienstleister allerdings eine große Herausforderung sein. Alternativ formuliert Artikel 49 DSGVO Ausnahmefälle, in denen eine Datenübertragung in ein Drittland erfolgen kann. Diese sind jedoch nicht für den Regelbetrieb vorgesehen und die Bedingungen eng begrenzt.

Vitako-Empfehlungen:

Sofern keine Alternativen zu bestimmten Diensten, die personenbezogene Daten in die USA übertragen, existieren, sollten entsprechend die oben beschriebenen Optionen genutzt werden. Dabei empfiehlt es sich in jedem Fall, den Rat der Datenschutzbeauftragen einzuholen.

Grundsätzlich sollte für alle Anwendungen, bei denen Daten in Drittländer übertragen werden, die keinen Datenschutz nach europäischem Niveau bieten, geprüft werden, ob Alternativen zur Verfügung stehen, bei denen alle personenbezogenen Daten in der Europäischen Union verbleiben oder nur in Länder übertragen werden, für die ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt. Der LfDI des Landes Baden-Württemberg droht sogar an, Datenübertragungen zu untersagen, sollte nicht überzeugend dargelegt werden können, dass nicht auf solche Alternativen zurückgegriffen werden kann.

Für viele Basisanwendungen stehen auch Open-Source-Lösungen zur Verfügung, die im eigenen Rechenzentrum oder bei einem kommunalen IT-Dienstleister gehostet werden können. Hier ist die vollständige Kontrolle über alle Daten jederzeit gegeben.