Never Endig Story: Microsoft 365 und der Datenschutz

„Auf Grundlage des neuen EU-US Data Privacy Frameworks können Daten frei und sicher zwischen der EU und teilnehmenden US-Unternehmen fließen.“ Diese und ähnliche Aussagen werden Sie schnell finden, wenn Sie im allwissenden Internet nach der Möglichkeit recherchieren, (Cloud-)Dienste US-amerikanischer Anbieter für die Verarbeitung personenbezogener Daten zu nutzen. Warum dies so pauschal nicht korrekt ist soll mein folgender Newsletter aufzeigen. Und natürlich geht es hierbei nicht nur um Microsoft 365, sondern um das gesamte Spektrum der Software, die von Anbietern in den USA bereitgestellt werden.

Zum besseren Verständnis: Etwas Geschichte zum Thema

Juli 2000	Wir befinden uns noch vor dem Inkrafttreten der EU-DSGVO, es gilt entsprechende EU-Richtlinie zur Umsetzung in nationales Recht und damit das BDSG (alt). Mit dem Safe-Harbor-Abkommen zwischen den USA und der EU soll eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten aus der EU in den USA geschaffen werden. US-amerikanische Unternehmen konnten sich in eine Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichtet haben, bestimmte datenschutzrechtliche Anforderungen („Safe Harbour Principles“) zu erfüllen.
2015-10-06	Durch ein EuGH-Urteil (heute nach dem Kläger häufig als Schrems-I-Urteil bezeichnet) wird das Safe-Harbour-Abkommen für ungültig erklärt. Von einem Tag auf den nächsten wäre damit die Rechtsgrundlage für sämtliche Auftragsverarbeitungen europäischer Unternehmen in den USA entfallen. Die Datenschutz-Aufsichtsbehörden der EU einigten sich daher auf eine Übergangsfrist bis 2016-01-31.
2016-02-01	Die Übergangsfrist ist abgelaufen, die meisten Datenverarbeitungen von EU-ansässigen Unternehmen in den USA hätten sofort eingestellt werden müssen. Wer seine Prozesse nicht entsprechend anpassen und die Verarbeitung in den Geltungsbereich der EU-Richtlinie verlagern konnte war ab sofort dem Risiko von Bußgeldern ausgesetzt.
2016-07-12	Das Nachfolgeabkommen „EU-US Privacy Shield“ tritt in Kraft. Es sah vor, dass unter bestimmten Voraussetzungen (u. a. bei der Verwendung von sogenannten Standardvertragsklauseln für Auftragsverarbeitung) die Verarbeitung personenbezogener Daten in den USA möglich ist. Von Beginn an wurden jedoch Zweifel laut, ob der EU-US Privacy Shield den Anforderungen der mittlerweile formulierten, aber noch nicht in Kraft getretenen EU-DSGVO genüge tut. Die bis dahin verwendeten Standardvertragsklauseln waren bereits 2015[1]) und abermals 2020[2]) für nicht mehr

[1]) Urteil vom 2015-10-06
[2]) Urteil vom 2020-07-16 (Rechtssache C-311/18, sogenanntes Schrems-II-Urteil)

Volker Baron (Dipl.-Geograph / IT-Systemelektroniker) – **Tel.:** +49 89 18923500 – **Fax:** +49 89 18923501
Büro: Haydnstraße 2, 80336 München – **E-Mail:** volker.baron@baron-consult.de – **Internet:** www.baron-consult.de
Finanzamt München I, USt-ID: DE 216791626
Bankverbindung: Münchner Bank eG, IBAN: DE84 7019 0000 0000 3389 15, BIC: GENODEF1M01

anwendbar erklärt, da die geforderten datenschutzrechtlichen Zusicherungen in Ländern mit gegenläufigen Rechtsbestimmungen gar nicht abgegeben werden können.

2018-05-25 Endgültiges Inkrafttreten der EU-DSGVO nach einer zweijährigen Übergangsfrist. In Artikel 28 finden sich grundlegende Anforderungen an Auftragsverarbeiter und an die mit diesen zu schließenden Verträge. Die Datenverarbeitung von EU-Unternehmen in den USA ist damit abermals mit (jetzt deutlich höheren) Bußgeldern bewährt.

2021-06-04 Wegen der großen Relevanz des Themas für viele im Geltungsbereich der EU-DSGVO ansässige Unternehmen versucht die EU-Kommission abermals, eine Rechtsgrundlage für Datenverarbeitungen in sogenannten „Drittländern“[3]), also auch in den USA, zu schaffen: Unter dem Namen „EU-U.S. Data Privacy Framework“ werden abermals Voraussetzungen formuliert, unter denen eine Übertragung personenbezogener Daten in den USA stattfinden kann. Nach den beiden Rückschlägen zum Safe-Harbour-Abkommen und zum EU-US Privacy Shield sind die Anforderungen jedoch deutlich gewachsen, so dass – zumindest für kleinere und mittlere Betriebe – die Frage nach der Verhältnismäßigkeit gestellt werden muss. So ist beispielsweise vor der Aufnahme einer Datenübertragung und -verarbeitung eine Datenschutz-Folgenabschätzung nach Art. 35 EU-DSGVO durchzuführen.

2023-07-10 Annahme des neuen Angemessenheitsbeschlusses EU-U.S. Data Privacy Framework durch die EU-Kommission.

Das EU-U.S. Data Privacy Framework (DPF)

Handelte es sich bei dem Safe-Harbour-Abkommen noch um eine Verpflichtungserklärung der teilnehmenden U.S.-Unternehmen, so wurden für das DPF umfangreiche Verhandlungen mit Regierungsorganisationen in den USA geführt, um dort eine entsprechende Rechtsgrundlage (Executive Order 14086) zu schaffen[4]). Damit soll das Argument der Beschwerdeführer aus den beiden Schrems-Urteilen entkräftet werden, dass ein in den USA ansässiges Unternehmen die geforderten Zusicherungen auf Grund der dort geltenden Rechtslage gar nicht abgeben kann.

Die Berufung darauf, dass das mit der Auftragsverarbeitung betraute Unternehmen am DPF teilnimmt reicht rechtlich jedoch bei weitem nicht aus, um personenbezogene Daten zu übermitteln und zu verarbeiten:

Das U.S.-amerikanische Unternehmen muss sich jährlich rezertifizieren lassen und kann andernfalls aus der Liste[5]) der vom DPF begünstigten Unternehmen gestrichen werden. Vom Verantwortlichen

---

[3]) Als Drittländer werden alle Länder angesehen, die nicht einem der folgenden Kriterien entsprechen:
- Mitglied in der Europäischen Union (EU)
- Mitglied im Europäischen Wirtschaftsraum (EWR)
- Von der EU-Kommission nach Art. 45 EU-DSGVO in die Liste der Staaten mit gleichwertigem Datenschutzniveau aufgenommen (z. B. Israel, Schweiz). Die auf der Liste benannten Länder werden periodisch überprüft, so dass der Verantwortliche regelmäßig prüfen sollte, ob das Zielland einer Datenübertragung noch enthalten ist. Andererseits können auch weitere Länder in die Liste aufgenommen werden, wenn die EU-Kommission nach Prüfung zu dem Ergebnis kommt, dass diese über ein gleichwertiges Datenschutzniveau verfügen.

[4]) Im „Agreement in principle for a Trans-Atlantic Data Privacy Framework“ vom März 2020 heißt es hierzu: „A new set of rules and binding safeguards to limit access to data by U.S. intelligence authorities to what is necessary and proportionate to protect national security; U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards“

[5]) Die Liste kann unter dem folgenden Link eingesehen werden: https://www.dataprivacyframework.gov/s/participant-search

muss also periodisch geprüft werden, ob das beauftragte Unternehmen noch am DPF teilnehmen kann.

Dem Verantwortlichen obliegt es, genau zu prüfen, ob ggf. auch die beauftragte Untergliederung eines U.S.-amerikanischen Unternehmens zertifiziert ist. So findet man bei der Recherche nach „Microsoft“ den Hinweis auf 18 weitere Tochtergesellschaften („Entities“), die durch das DPF gedeckt sind. Ist die von Ihnen beauftragte Untergliederung aber wirklich dabei?

Dass ein U.S.-amerikanisches Unternehmen am DPF teilnimmt entbindet nicht davon, mit diesem Unternehmen einen Vertrag zur Auftragsverarbeitung abzuschließen. Die EU-Kommission hat hierzu Standardvertragsklauseln definiert, deren Inhalt jedoch auf die jeweilige Verarbeitungssituation angepasst werden muss. Die Kanzlei WBS.LEGAL Rechtsanwaltsgesellschaft mbH & Co. KG bietet auf ihrer Website beispielsweise vorausgefüllte Verträge an, die nach eigenen Angaben den Anforderungen der meisten Unternehmen entsprechen. Doch wird sich ihr Vertragspartner, der sicher lieber seinen eigenen Vertragstext verwendet, auf dieses Muster einlassen? Und wenn ja, wird er Ihnen die juristische Prüfung ihres Entwurfs in Rechnung stellen?

Auch bei Verarbeitungen im Rahmen des DPF gilt der Grundsatz der Datensparsamkeit. Konkret heißt dies, dass es dem Verantwortlichen obliegt, z. B. das von ihm eingesetzte Office 365 so zu konfigurieren, dass überflüssige Datenerhebungen und -übermittlungen unterbleiben. Dies würde prinzipiell auch dann gelten, wenn das Softwareprodukt ausschließlich lokal auf Hardware des Verantwortlichen installiert wird. Bei Cloud-Lösungen ist die datenschutzkonforme Konfiguration erfahrungsgemäß jedoch schwieriger, da hier (beinahe) jede Datenerfassung einen Datentransfer zum Anbieter der Software auslöst. Ihr IT-Administrator mag ein Meister seines Faches sein. Aber ist er auch Spezialist für die gewählte Cloud-Lösung?

Kritik und Bedenken

Im Zertifizierungsprofil der am DPF teilnehmenden Unternehmen werden die Zwecke der eigenen Datenverarbeitungen benannt („Purpose of Data Collection“), jedoch teilweise nur in sehr allgemein gehaltenen Formulierungen. Im Rahmen einer Datenschutz-Folgenabschätzung ist eine Risikobewertung daher nur bedingt möglich. Auch die im Abschnitt „Privacy Policy“ verlinkten Datenschutzerklärungen der Unternehmen können nur mit großem Aufwand für eine Prüfung herangezogen werden, weil sie alle Produkte des Unternehmens umfassen, die beauftragten Leistungen jedoch einzeln bewertet werden müssen.

Eine erste Klage gegen den Angemessenheitsbeschluss im Rahmen des DPF hat es bereits gegeben: Die Klage des französischen EU-Parlamentariers Philippe Latombe auf Nichtigerklärung des DPF wurde jedoch abgewiesen.

Doch auch die Datenschutzorganisation von Herrn Schrems NYOB ist schon wieder aktiv. Gegen die Schulversion Microsoft 365 Education wurden bereits zwei Beschwerden[6]) bei der Österreichischen Datenschutzbehörde eingereicht. Die Beschwerden stellen zwar nicht die prinzipiellen Regelungen des DPF in Frage, sie richten sich jedoch dagegen, dass Microsoft 365 Education trotz der Zertifizierung des Anbieters nicht den Datenschutzregelungen in der EU entspricht. Konkret handelt es sich um die Nichterfüllung von Auskunftsersuchen des Anbieters, um

[6]) beide Beschwerden vom 2024-06-04

die Verwendung von Tracking-Cookies ohne Einwilligung des Betroffenen und die Nichterfüllung von Informationspflichten. Beachtlich ist hierbei, dass im Falle einer der beiden Beschwerden nicht nur die Microsoft Corporation in den USA, sondern auch die Bildungsdirektion Wien und das österreichische Bundesministerium für Bildung, Wissenschaft und Forschung als Beschwerdegegnerinnen benannt sind.

Darüber hinaus hat NYOB angekündigt, auch gegen das DPF vorgehen zu wollen.

Konkrete Empfehlungen

An der Nutzung von Software und Online-Diensten US-amerikanischer Anbieter kommt man nur schwer vorbei, zum einen, weil diese Anbieter mit ihrer Software weltweite Standards gesetzt haben, zum anderen, weil es für bestimmte Anforderungen nur wenige oder keine in der EU ansässige Anbieter gibt. Ein Beispiel ist hier Microsoft Exchange, das in Verbindung mit unterschiedlichsten Mailprogrammen plattformübergreifend eine volle Synchronisation des gesamten Mailverkehrs, des Kalenders, der Kontakte und von Notizen ermöglicht. Wer also die Software eines US-amerikanischen Anbieters nutzen möchte bzw. muss sollte die folgenden Empfehlungen beherzigen:

- Prüfen Sie, ob es zumutbare Alternativen zu dem gewünschten System gibt. Vielleicht bietet ein im Geltungsbereich der EU-DSGVO ansässiges Unternehmen eine vergleichbare Lösung an. Dies gilt insbesondere, wenn besondere Kategorien personenbezogener Daten nach Art. 9 EU-DSGVO verarbeitet werden sollen.
- Überlegen Sie genau, welche Daten Sie über das gewählte System verarbeiten wollen. Es gilt hier mehr denn sonst das Prinzip der Datensparsamkeit.
- Prüfen Sie, ob der Anbieter auf der Liste der DPF-zertifizierten Unternehmen steht. Legen Sie eine Wiedervorlage für die erneute Überprüfung an.
- Setzen Sie nicht auf „datenschutzfreundliche Voreinstellungen“ in der eingesetzten Software. Ziehen Sie einen sachkundigen IT-Administrator (m/w/d) hinzu und stimmen Sie im Zweifel die Konfiguration mit Ihrem Datenschutzbeauftragten ab.
- Schließen Sie mit dem Anbieter einen Vertrag zur Auftragsverarbeitung.
- Nehmen Sie vor der ersten Datenübermittlung das gewählte System in das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO auf. Dokumentieren Sie ausführlich die Zwecke der Verarbeitung, die Kategorien betroffener Personen und die Kategorien personenbezogener Daten, die Empfänger der Daten, die durchgeführte Überprüfung der DPF-Zertifizierung, Vorgehensweise und Fristen für die Datenlöschung sowie die getroffenen technisch-organisatorischen Maßnahmen für eine sichere Datenübermittlung und Verarbeitung.
- Handelt es sich bei der eingesetzten Software um einen öffentlich zugänglichen Dienst, z. B. weil diese in eine Internetpräsenz eingebunden ist, muss die Datenschutzerklärung angepasst werden. Der Hinweis auf die Verarbeitung in einem „unsicheren Drittland“ kann entfallen bzw. durch den Hinweis auf das DPF ersetzt werden. Aber bitte nicht verwechseln: Handelt es sich um eine Datenverarbeitung, die für die Bereitstellung des Dienstes technisch nicht unbedingt erforderlich ist (vgl. hierzu § 25 TDDDSG) bzw. auf eine der Rechtsgrundlagen nach Art. 6 Abs. 1 EU-DSGVO gestützt werden kann, bleibt diese auch weiterhin einwilligungspflichtig.

Und hier noch ein persönlicher Tipp von mir: Überlegen Sie bereits jetzt wie Sie vorgehen wollen, wenn das beauftragte Unternehmen aus der Liste der DPF-zertifizierten Unternehmen herausfällt oder das DPF aufgrund einer erneuten Klageerhebung vor dem EuGH als Rechtsgrundlage für die Beauftragung eines Unternehmens im „unsicheren Drittstaat“ USA entfällt.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

München, 2024-08-11

Volker Baron