INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

Univ.-Prof. Dr. Dirk Heckmann

Cloud Computing und Datenschutzrecht

Rechtliche Herausforderungen bei der Einbindung US-amerikanischer Anbieter

KURZGUTACHTEN MIT HANDLUNGSEMPFEHLUNGEN

INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

Stiftungsvorstand
Rudolf Schleyer, AKDB
Gudrun Aschenbrenner, AKDB

Kuratorium
Dr. Franz Dirnberger, Bayerischer Gemeindetag
Bernd Buckenhofer, Bayerischer Städtetag
Dr. Johann Keller, Bayerischer Landkreistag
Stefanie Krüger, Bayerischer Bezirketag

IMPRESSUM

Herausgeber
Innovationsstiftung Bayerische Kommune
c/o Anstalt für Kommunale Datenverarbeitung in Bayern – AKDB
Hauptverwaltung
Hansastraße 12-16
80686 München
Postfach 150140
80042 München

© Innovationsstiftung Bayerische Kommune, München 2020
www.bay-innovationsstiftung.de

Univ.-Prof. Dr. Dirk Heckmann

Cloud Computing und Datenschutzrecht

Rechtliche Herausforderungen bei der Einbindung US-amerikanischer Anbieter

Kurzgutachten

mit Handlungsempfehlungen vom 19.6.2020

Inhaltsverzeichnis

I. Nutzung von IT-Produkten US-amerikanischer Anbieter 7

II. Ausgangslage Cloud-Nutzung im Lichte des Datenschutzrechts 8

III. Rechtliche Bewertung von cloud-basierten IT-Produkten US-amerikanischer Anbieter 10

1. Cloud-Dienste US-amerikanischer Anbieter und DSGVO 10

2. Rechtslage in den USA 13

3. Microsoft-Case 14

4. Änderungen im Zuge des CLOUD-Acts 15

5. Nutzerseitige Verschlüsselung oder Pseudonymisierung als Lösung? 16

IV. Erhebung und Versendung von Telemetriedaten bei MS Office 365 18

V. Erhebung und Versendung von Telemetriedaten bei MS Windows 10 21

VI. Technisch-organisatorischer Datenschutz 24

VII. Fazit 27

ANHANG: Exkurs zum Cloud Treuhandmodell Microsoft Cloud Deutschland 30

Executive Summary und Handlungsempfehlungen

1. Sowohl private Unternehmen und Verbraucher als auch Behörden auf allen Ebenen nutzen in der Praxis vielfach cloud-basierte Softwarelösungen wie Microsoft Windows 10 oder Microsoft 365 (früher: Office 365), weil dies einen hohen Nutzen und Effizienzvorteile und auch eine hohe Interoperabilität innerhalb etablierter IT-Umgebungen verspricht. In der Corona-Krise gilt, was normalerweise innovationsfeindlich wirkt: „never change a running system".

2. Weil und soweit solche IT-Produkte von US-amerikanischen Anbietern stammen, wirft dies besondere datenschutzrechtliche Fragen auf. Aufgrund verschiedener US-amerikanischer Rechtsvorschriften (insbesondere dem CLOUD-Act) können US-Behörden zum Zugriff auf Daten berechtigt sein, die auf Servern der Cloud-Anbieter gespeichert sind (auch wenn sich die Server nicht in den USA, sondern in Deutschland befinden) Schon eine passive Bereithaltungspflicht kann mit einer datenschutzrechtlichen Übermittlung in ein „unsicheres Drittland" gleichzusetzen sein.

3. Datenschutzrechtliche Herausforderungen ergeben sich auch aus dem Gesichtspunkt der automatischen Erhebung und Verarbeitung von Telemetrie-/Diagnosedaten in einem Betriebssystem wie Windows 10.

4. Vor diesem Hintergrund wird schon seit längerer Zeit bezweifelt, ob insbesondere öffentliche Stellen überhaupt Cloud-Dienste US-amerikanischer Anbieter nutzen dürfen.

5. Während die Datenschutzaufsichtsbehörden in einzelnen Bundesländern erwägen, die Nutzung zu untersagen, hat sich die Datenschutzkonferenz auch nach jahrelanger Befassung noch nicht zu einem klaren Votum durchgerungen. So gibt es zwar ein „Prüfschema zum datenschutzkonformen Betrieb von Windows 10"[1], aber weder ein bundeseinheitlich wirksames „Verbot" bei Nichteinhaltung dieses Prüfschemas noch eine verbindliche Aussage zu „Office 365"[2].

6. Die Rechtsunsicherheit, die letztlich auch durch die Datenschutzaufsichtsbehörden nicht beseitigt wird, darf weder zu Lasten der Anwender noch der schützenswerten Daten der Bürger gehen. Es liegt deshalb nahe, in dieser speziellen Frage von einer zumindest vorübergehenden Duldung der Nutzung der genannten Cloud-Angebote auszugehen. Eine solche Duldung begründet keinen weitergehenden Bestands- und Investitionsschutz: Die Anwender können angesichts der offenen Diskussion um die Datenschutzkonformität

[1] https://www.datenschutzkonferenz-online.de/media/ah/20191106_win10_pruefschema_dsk.pdf. Weitergehende technische Aspekte sind in einer Anlage ausgeführt: https://tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/beschluss_zu_top_10_win_10_prufschema_anlage.pdf

[2] So heißt es in im Beschluss der Datenschutzkonferenz vom 6./7.11.2019 zu TOP 34 („Office 365") „Die Konferenz kommt überein, den von Brandenburg eingebrachten Beschlussvorschlag zunächst an den UAK Office 365 zu verweisen. Dieser wird um die Erarbeitung einer abgestimmten und begründeten Bewertung einer datenschutzkonformen Auftragsverarbeitung von Office 365 gebeten. Die Arbeitskreise Verwaltung, Technik, Schulen und Bildungseinrichtungen sollen hierbei einbezogen werden." https://www.datenschutzkonferenz-online.de/media/pr/20201114_protokoll_98_dsk.pdf

nicht auf eine langfristige Nutzung rechtlich fragwürdiger Cloud-Angebote vertrauen, sollten sich zumutbare Alternativen hierzu ergeben, die sich in einer Gesamtabwägung als vorzugswürdig erweisen.

7. Umgekehrt besteht für die Nutzer eine Obliegenheit zu

- kontinuierlicher Beobachtung der Stellungnahmen der Datenschutzkonferenz
- Einhaltung von Vorgaben der Datenschutzkonferenz wie dem „Prüfschema zu Windows 10“ (so weit wie möglich)
- Suche nach alternativen Cloud-Lösungen und Prüfung der Zumutbarkeit ihrer Implementierung, insbesondere unter haushaltsrechtlichen, wirtschaftlichen und technisch-organisatorischen Aspekten
- weitgehender Beachtung von Drittinteressen, vor allem die der Bürgerinnen und Bürger, deren Daten verarbeitet werden, sowie
- Dokumentation der getroffenen Entscheidung und ihrer Begründung.

8. Unter Einhaltung dieser Verfahrensvorkehrungen wären datenschutzrechtliche Sanktionen wohl widersprüchlich und unzulässig („venire contra factum proprium“).

9. Dies gilt in erster Linie für latent alternativlose Standardsoftware mit einer hohen Marktdurchdringung. Außerhalb dessen (etwa bei Cloud-Diensten deutscher Anbieter im E-Government) können sich hingegen zumutbare Alternativen ergeben, insbesondere bei der insoweit unproblematischen Inanspruchnahme öffentlich-rechtlicher IT-Dienstleister oder kommunaler bzw. Landesrechenzentren.

I. Nutzung von IT-Produkten US-amerikanischer Anbieter

In jüngster Zeit verstärkt sich die Diskussion darüber, ob nach geltendem Datenschutzrecht die Einbindung von cloud-basierten IT-Produkten des US-amerikanischen Anbieters Microsoft, u.a. Office 365 (nunmehr: Microsoft 365) oder Windows 10, durch deutsche Kommunen und Behörden zulässig sein kann. Streitpunkte bestehen hier insbesondere hinsichtlich einer geeigneten Rechtsgrundlage für die Datenverarbeitung, der Erhebung und Versendung von sog. Telemetriedaten und die grundsätzliche (potenzielle) Übermittlung von Daten in die USA.

Die Aufsichtsbehörden sind sich bei der Einschätzung des Einsatzes der Produkte Office 365 (Microsoft 365) und Windows 10 aber keineswegs einig[3]. Anfang Juli 2019 hatte etwa der hessische Datenschutzbeauftragte – im Anschluss an die Rechtsauffassung der Datenschutzaufsicht in Schleswig-Holstein[4] – die Absicht, den Einsatz Cloud-basierter[5] Anwendungen in Schulen vollständig zu untersagen;[6] insbesondere den Einsatz von Microsoft Office 365 stufte der Datenschutzbeauftragte als datenschutzrechtlich unzulässig ein.[7] Anfang August 2019 sprach sich der oberste Datenschützer in Hessen dann doch für eine Duldung des Softwareeinsatzes aus: vorbehaltlich einer weiteren Überprüfung würden hinsichtlich der Versionen Office 365 ProPlus, Office 365 Online und Office365 Apps keine Aufsichtsmaßnahmen geltend gemacht. Dabei wurde Schulen, die sich nach Veröffentlichung der Stellungnahme zum Einsatz von MS Office entscheiden, ausdrücklich aber kein Vertrauensschutz eigeräumt.[8]

---

[3] Inzwischen hat die Datenschutzkonferenz jedoch immerhin ein Prüfschema zum datenschutzkonformen Betrieb von Windows 10 erstellt. Abrufbar unter: https://lfd.niedersachsen.de/startseite/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/datenschutzkonformer_einsatz_von_windows_10/positionierung-der-dsk-zum-datenschutzkonformen-einsatz-von-windows-10-177265.html.

[4] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, abrufbar unter https://www.datenschutzzentrum.de/tb/tb35/kap07.html.

[5] In der weiteren Darstellung werden die Begriffe Cloud und Cloud-basiert einheitlich verwendet.

[6] Vgl. *Crolly,* Welt, https://www.welt.de/wirtschaft/article197952453/DSGVO-Schulen-bei-Office-365-Einsatz-in-Rechtsunsicherheit.html.

[7] *Hessischer Beauftragte für Datenschutz und Informationsfreiheit,* Stellungnahme zum Einsatz von Microsoft Office 365, https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und.

[8] *Hessischer Beauftragte für Datenschutz und Informationsfreiheit,* Zweite Stellungnahme zum Einsatz von Microsoft Office 365, https://datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen. Beim Einsatz dieser Produkte soll allerdings die Übermittlung von Diagnosedaten jedweder Art unterbunden werden (siehe hierzu noch unten). Vgl. auch *Krempl,* heise, https://www.heise.de/newsticker/meldung/Datenschuetzer-duldet-Microsoft-Office-365-nun-doch-teilweise-an-Schulen-4490044.html.

In ähnlicher Weise wurde bereits in einer Studie, die das niederländische Justizministerium in Auftrag gegeben hatte, der Einsatz von Microsoft Office 365 für datenschutzrechtlich bedenklich eingestuft.[9] Im Vordergrund stand auch hier die Erhebung und Übermittlung sogenannter Diagnose- bzw. Telemetriedaten. Nach ersten Gesprächen mit Microsoft und einer umfassenden Transparenzoffensive des Unternehmens hinsichtlich der Erhebung von Diagnosedaten, geht aus einem Schreiben des niederländischen Innenministers und des Justizministers an das Parlament hervor, dass sich die Niederlande und Microsoft auf zusätzliche Datenschutzvorkehrungen geeinigt hätten, die einen datenschutzkonformen Einsatz von Microsoft Office 365 und Windows 10 nun ermöglichten.[10]

Anlässlich der weiterhin ungeklärten Rechtsfragen zum Einsatz cloud-basierter IT-Anwendungen, insbesondere von Microsoft Office 365 und Windows 10, ist eine Aufbereitung der Streitfragen und die Entwicklung von Lösungsansätzen angezeigt. Dies gilt um so mehr, als Microsoft sein Office Angebot perspektivisch nur noch aus der Cloud anbietet, so dass das Thema mangels Alternative on premise eine besondere Brisanz gewinnt. Werden Anwender (vom privaten Nutzer über Unternehmen bis zu Behörden) gleichsam „in die Cloud gezwungen", weil das gesamte „Ökosystem" von Standardprogrammen wie Textverarbeitung, Tabellenkalkulation etc. als Cloud-Lösung konzipiert ist.

II. Ausgangslage Cloud-Nutzung im Lichte des Datenschutzrechts

Das sog. Safe Harbor-Urteil des EuGH vom 6.10.2015 (C-362/14), hatte bei vielen Unternehmen, aber auch Behörden und anderen Institutionen für Rechtsunsicherheit gesorgt: Inwieweit war es nunmehr überhaupt erlaubt, Cloud Computing Dienste US-amerikanischer Anbieter in Anspruch zu nehmen, wurden dabei doch zumeist Daten auch auf amerikanischen Servern (also aus datenschutzrechtlicher Sicht: in einem (unsicheren) Drittstaat) zumindest vorübergehend gespeichert? Das Safe-Harbor-Abkommen wurde mittlerweile durch den EU-US-Privacy Shield abgelöst, der seinerseits umstritten ist.[11] Das

[9] *Nas/Roosendaal*, Privacy Company, Microsoft Office Pro Plus Studie, November 2018, abrufbar unter: https://www.privacycompany.eu/en/impact-assessment-shows-privacy-risks-microsoft-office-proplus-enterprise/ (Microsoft Pro Plus Studie).

[10] *VITAKO,* https://206182.seu2.cleverreach.com/m/11492257/560141-c8a550f41b055209828ab4b36b129677.

[11] Der Generalanwalt beim EuGH hat in seinem Schlussantrag in Sachen „Schrems II" erhebliche Bedenken gegen den Privacy Shield angemeldet: https://netzpolitik.org/2019/eu-generalanwalt-gibt-schrems-in-facebook-fall-recht/. Das Urteil des EuGH wird im Laufe des Jahres 2020 erwartet.

Europäische Parlament hat erst am 05. Juli 2018 eine kritische Resolution bzgl. des Privacy Shields verfasst, nachdem es Defizite bei der Einhaltung der notwendigen Datenschutzstandards auf amerikanischer Seite festgestellte.[12] Kernproblem der Nutzung von IT-Produkten US-amerikanischer Anbieter ist hierbei stets die (potenzielle) Übermittlung von in Deutschland erhobenen Daten an die in den USA ansässigen Unternehmen oder dort zuständige Ermittlungsbehörden.

Einige (bisherige) Cloud Angebote US-amerikanischer Anbieter wie Microsoft oder Amazon sind dezidiert an den deutschen Markt adressiert und sollen ein hohes Datenschutzniveau dadurch garantieren, dass ausschließlich in Deutschland (oder ggf. anderen EU-Mitgliedstaaten) gelegene Server verwendet werden.

Bis vor kurzem versprach die Microsoft Corporation ihren Kunden hierzulande sogar mit ihrer „deutschen" Cloud die Daten über ein von der globalen Infrastruktur getrenntes Netzwerk zu speichern und die vollständige Kontrolle über die Daten einem Datentreuhänder zu überlassen.[13] Dieses Vorgehen sollte garantieren, dass die Daten gegen den etwaigen Zugriff von US-(Sicherheits-)Behörden sicher sind. 2019 ist dieses „Deutschland-Cloud"-Angebot allerdings eingestellt worden, nach Aussage des Unternehmens aufgrund mangelnder Nachfrage.[14] Inzwischen bietet Microsoft einen ähnlichen Dienst wieder in Deutschland an. Daten deutscher Kunden werden auf Servern in Deutschland gespeichert, sind aber trotzdem in das weltweite Cloud-Netzwerk von Microsoft eingebunden.[15]

Vor dem Hintergrund kritischer Stimmen aus den Datenschutzbehörden[16] untersucht dieses Rechtsgutachten die allgemeine rechtliche Lage zur Nutzung US-amerikanischer Cloud-Angebote. Anschließend soll die technische und rechtliche Situation des Einsatzes von Microsoft Office 365 (nun: Microsoft 365) und Windows 10 dargestellt werden. Hierbei wird geklärt, ob und inwieweit deutsche Kommunen diese Produkte aus datenschutzrechtlicher Sicht verwenden dürfen.

---

[12] *Europäisches Parlament*, http://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_DE.html.
[13] *Microsoft,* https://news.microsoft.com/de-de/microsoft-cloud-2019-rechenzentren-deutschland/.
[14] Vgl. *Spiegel Online,* https://www.spiegel.de/netzwelt/web/deutsche-cloud-microsoft-stellt-vertrieb-seines-datendienstes-ein-a-1226307.html.
[15] Vgl. etwa *heise,* https://www.heise.de/newsticker/meldung/Microsoft-erweitert-sein-deutsches-Cloud-Angebot-4665168.html. Dieser Artikel zeigt auch in Teilen auf in welchen Ländern welche Daten gespeichert werden, jedoch scheint Microsoft hier nicht sehr transparent zu sein.
[16] Vgl. etwa *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,* welches zu dem Schluss kommt, dass Microsoft Office 365 nicht geeignet ist, personenbezogene Daten datenschutzkonform zu verarbeiten, abrufbar unter https://www.datenschutzzentrum.de/tb/tb35/kap07.html.

III. Rechtliche Bewertung von cloud-basierten IT-Produkten US-amerikanischer Anbieter

Werden Cloud-Angebote genutzt, so handelt es sich überwiegend um die Speicherung, also eine Verarbeitung (Art. 4 Nr. 2 DSGVO) personenbezogener Daten.[17] Ist dies der Fall, so bestimmt sich die rechtliche Zulässigkeit der Cloud-Nutzung maßgeblich nach den Vorgaben der Datenschutzgrundverordnung, vgl. Art. 1 Abs. 1 DSGVO. Die Verarbeitung darf zunächst nur aufgrund einer Einwilligung der betroffenen Person oder weiteren, von der DSGVO vorgegebenen Rechtsgrundlagen erfolgen, Art. 6 DSGVO. Ist eine Verarbeitung aufgrund einer einschlägigen Grundlage rechtmäßig, so gelten für die Einbeziehung Dritter, in diesem Fall des Cloud-Anbieters die weiteren Bestimmungen der Art. 28, 29 DSGVO und bei Datenübermittlungen an Drittländer Art. 44 ff. DSGVO.

1. Cloud-Dienste US-amerikanischer Anbieter und DSGVO

Wenn ein Unternehmen mit Sitz in der Bundesrepublik Deutschland einen Cloud-Dienst bei der Verarbeitung personenbezogener Daten in Anspruch nimmt, bleibt das Unternehmen weiterhin Verantwortlicher im Sinne der Datenschutzgrundverordnung und somit Adressat der datenschutzrechtlichen Bestimmungen, vgl. Art. 4 Nr. 7 DSGVO. Für das Unternehmen bedeutet dies, dass es dem Betroffenen gegenüber haftet[18], wenn dessen Daten in der Cloud verloren gehen oder gar missbraucht werden.

Zwischen dem Unternehmen mit Sitz in Deutschland und Microsoft/dem amerikanischen Cloud-Anbieter besteht regelmäßig ein Auftragsverarbeitungsverhältnis gem. Art. 28 DSGVO[19]. Dies jedoch nur insofern, als der Auftraggeber als Verantwortlicher die Bestimmungshoheit über Art und Maß der Datenverarbeitung aufrechterhält, vgl. Art. 4 Nr. 7 und 8, Art. 28 Abs. 3 a) DSGVO (Weisungsgebundenheit). Letzteres gestattet die Übermittlung personenbezogener Daten an den Auftragsverarbeiter, wenn der Auftrag schriftlich (auch in einem elektronischen Format) erteilt wurde (Art. 28 Abs. 9 DSGVO), und die weiteren Vertragsbestandteile nach Maßgabe des Art. 28 Abs. 3 DSGVO geregelt werden. Das deutsche Unternehmen muss also vor allem weisungsbefugt bleiben (Art. 28 Abs. 3 a) DSGVO). Sind alle Voraussetzungen erfüllt, ist der Cloud-Anbieter als Auftragsverarbeiter nicht

[17] *Bräutigam/Thalhofer,* in: Bräutigam, IT-Outsourcing und Cloud-Computing, 4. Auflage 2019, S. 1275.
[18] Die Haftung nach der Datenschutzgrundverordnung wird in Art. 82 DSGVO geregelt. Auch eine Haftung aus dem Deliktsrecht (etwa § 823 Abs. 2 BGB i. V. m. DSGVO-Schutzgesetz) ist denkbar, Für öffentliche Stellen kommt zusätzlich der Amtshaftungsanspruch aus § 839 BGB i.V.m. Art. 34 GG in Betracht.
[19] Vgl. auch *Gerlach* CR 2020, 165, 168.

„Dritter“ i.S.d. Art. 4 Nr. 10 DSGVO, wodurch seitens des Auftragsverarbeiters keine grundsätzlich erneut erlaubnispflichtige Verarbeitung[20] nach Art. 6 DSGVO vorliegt. Liegt hingegen eine gemeinsame Kontrolle über die Verarbeitung („Joint Control“) gem. Art. 26 DSGVO vor, so ist schon die Datenübermittlung an den Cloud-Anbieter gesondert rechtfertigungsbedürftig.[21]

Soweit zumindest die Theorie, also die normative Ausgangssituation. In der Praxis ist zu konzedieren, dass Verantwortliche bei US-amerikanischen Cloud-Anbietern keine realistische Chance haben, z.B. ihre Inspektionsrechte gem. Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO durchzusetzen. Folglich können etwa korrekte Datenübermittlungseinstellungen nicht wirksam überprüft werden. So können „Auftraggeber“ wie Kommunen Ihrer Pflicht zur Überprüfung und Bewertung der Wirksamkeit der technisch-organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nicht nachkommen. Die DSGVO hat – wie man auch an den ungelösten Fragen rund um das Safe-Harbor oder das EU US Privacy Shield Abkommen sieht – das Machtgefälle zwischen am Markt dominanten US-Unternehmen und ihren Kunden verdrängt.

Exkurs: Datenschutzrechtliche Relevanz der Weisungsbefugnis

Im Rahmen der Auftragsverarbeitung ist das Merkmal der Weisungsgebundenheit des Auftragnehmers zentral für die Einordnung als solche. Bestimmt tatsächlich der Cloud-Anbieter Art und Maß der Datenverarbeitung, so ist dieser nicht reiner Auftragnehmer, sondern mindestens mit dem Vertragspartner/Auftraggeber gemeinsam verantwortlich im Sinne des Art. 26 DSGVO. Die Beurteilung, ob eine Weisungsgebundenheit vorliegt, ist bei Cloud-Anbietern oftmals schwierig.[22] Zweck der Cloud-Nutzung ist gerade die Übernahme technischer und organisatorischer Maßnahmen durch den Cloud-Anbieter. Aufgrund der üblichen Standardisierung der Prozessabläufe wird in der Regel auch wenig Spielraum für den Auftraggeber bleiben, um die einzelnen Parameter der Verarbeitung festzulegen. Nicht zuletzt kann ein wirtschaftliches Ungleichgewicht zwischen Auftraggeber und Auftragnehmer dazu führen, dass die Bedingungen der Verarbeitung seitens des Cloud-Anbieters diktiert werden können.

Um der Rechtspraxis hingegen gerecht zu werden, lässt eine Vorverlagerung des Weisungszeitpunktes letztlich dennoch die Ansicht zu, dass ein Cloud-Anbieter weisungsabhängig im Sinne des Art. 28 Abs. 3 a) DSGVO ist. Soweit dem Auftraggeber die Wahl unterschiedlicher Cloud-Modelle zur Verfügung steht oder dieser über die Parameter des Cloud-Angebots umfangreich informiert wird (Transparenzerfordernis) und sich dann letztlich für die Nutzung dieses Angebots oder dagegen entscheidet, übt dieser seine Weisungsfreiheit im Rahmen der Vertragsfestsetzung bereits

[20] Auch die Übermittlung von Daten ist eine Verarbeitung im Sinne der DSGVO, Art. 4 Nr. 2, vgl. *Schild,* BeckOK Datenschutzrecht, 2019, DSGVO Art. 28, Rn. 29 f.

[21] *Bräutigam/Thalhofer,* in: Bräutigam, IT-Outsourcing und Cloud-Computing, 4. Auflage 2019, S. 1284.

[22] Vgl. *Bräutigam/Thalhofer,* in: Bräutigam, IT-Outsourcing und Cloud-Computing, 4. Auflage 2019, S. 1288 ff., so auch im Folgenden.

aus. Datenschutzwidrige Inhalte dürfen hierbei nicht Gegenstand der Auftragsvereinbarung werden.[23]
Zusätzlich sollten seitens des Cloud-Anbieters umfangreiche Informationen über die technischen und organisatorischen Maßnahmen im Sinne des Art. 32 DSGVO, die den Datenschutz gewährleisten sollen, zur Verfügung gestellt werden, um auch hier weitläufig Transparenz zu schaffen.
Darüber hinaus können allzu lange Vertragslaufzeiten zwar gegen das Vorliegen eines Weisungsverhältnisses sprechen, weil der Auftraggeber dann zu lange an seine ursprünglichen Weisungen gebunden wäre. Dem kann aber mit der Vereinbarung vereinfachter Möglichkeiten, sich vom Vertrag zu lösen, begegnet werden.[24]
Letztlich ist demnach zumindest im Rahmen des Vertragsschlusses und noch vor Beginn der tatsächlichen Cloud-Nutzung in besonderem Maße auf Transparenz und Entscheidungshoheit des Auftraggebers zu achten.[25]

Der Abschluss eines Vertrages nach Art. 28 DSGVO selbst genügt gleichwohl nur den Anforderungen der DSGVO, solange sich die Rechenzentren innerhalb der Europäischen Union befinden und die Datenverarbeitung ausschließlich dort stattfindet. Für die rechtskonforme Datenverarbeitung in sogenannten Drittstaaten[26], wozu auch die Vereinigten Staaten zählen, bedarf es mehr. Für die Übermittlung von Daten ins Ausland gilt, dass in dem betreffenden Drittland ein Datensicherheitsniveau entsprechend den Anforderungen der DSGVO gewährleistet sein muss, Art. 44 DSGVO. Grundlage der Übermittlung können geeignete Garantien sein (Art. 46 DSGVO). Zu diesen Garantien zählen unter anderem ein rechtlich bindendes Dokument zwischen Behörden oder öffentlichen Stellen (Art. 46 Abs. 2 a) DSGVO) oder verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 b) DSGVO). Letztere bedürfen zusätzlich der Genehmigung durch die zuständige Aufsichtsbehörde (Art. 47 Abs. 1 DSGVO). Darüber hinaus kann eine rechtmäßige Übermittlung auch auf Grundlage eines Angemessenheitsbeschlusses nach Art. 45 DSGVO erfolgen, demnach dem betreffenden Drittland ein angemessenes Schutzniveau bescheinigt wird. Beschlussberechtigt hierzu ist die Europäische Kommission (Art. 45 Abs. 1 S. 1 DSGVO). Länder, für die ein angemessenes Schutzniveau bereits anerkannt ist, sind z.B. Argentinien, Australien und Kanada.[27]

---

[23] *Bräutigam/Thalhofer,* in: Bräutigam, IT-Outsourcing und Cloud-Computing, 4. Auflage 2019, S. 1288 ff.
[24] *Bräutigam/Thalhofer,* in: Bräutigam, IT-Outsourcing und Cloud-Computing, 4. Auflage 2019, S. 1288f.
[25] Noch zur alten Rechtslage, bei der zur Bestimmung der Verantwortlichkeit ebenfalls die Weisungsgebundenheit entscheidendes Kriterium war, ist die Art. 29 Datenschutzgruppe pauschal von einer Auftragsdatenverarbeitung bei Beauftragung eines Cloud-Anbieters ausgegangen, vgl. Art. 29 Datenschutzgruppe, WP 169, S. 31.
[26] Bei diesen handelt es sich um Staaten außerhalb der EU und des Europäischen Wirtschaftsraums (EWR).
[27] Europäische Kommission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Im Verhältnis zu den USA kann seit dem 01.08.2016[28] eine Zertifizierung nach dem EU-US Privacy Shield zur Herstellung des entsprechenden Datenschutzniveaus vorgenommen werden. Ob der Angemessenheitsbeschluss der EU-Kommission zum Privacy Shield im Hinblick auf den US Patriot Act[29] und zuletzt die Executive Order[30] von Präsident Trump, insbesondere aber den CLOUD-Acts[31], allerdings bestehen bleibt, wird aktuell vor dem EuGH verhandelt. Den Angemessenheitsbeschluss bezüglich der Vorgängerversion des Privacy Shields, das Safe Harbor Abkommen, hatte der EuGH bereits für ungültig erklärt. Eine erneute Ungültigkeitserklärung durch den EuGH ist nicht auszuschließen.[32] Für den Fall, dass eine Ungültigkeitserklärung erfolgen sollte, geht etwa der Landesdatenschutzbeauftragte der Freien Hansestadt Bremen davon aus, dass die Datenübertragung, zumindest so wie bisher, unzulässig sein wird und rät zu Alternativmodellen.[33]
Unabhängig von der Frage des angemessenen Schutzniveaus, muss aus Unternehmens- beziehungsweise Behördensicht bei Einsatz der Cloud-Angebote geklärt werden, inwieweit die US-Administration Zugriff auf die Daten hat. Ein Herausgabeverlangen ist hierbei freilich nur unter den gesetzlich statuierten Anforderungen zulässig, unter anderem, wenn sich die herausverlangten Informationen physisch in den USA befinden und der herausgabepflichtige Dritte technischen Zugriff auf die Daten hat.[34] Fraglich ist dagegen, ob diese Herausgabepflicht auch dann besteht, wenn die Daten physisch außerhalb der USA gespeichert sind, der herausgabepflichtige Dritte aber eine faktische Zugriffsmöglichkeit besitzt.[35]

2. Rechtslage in den USA

Soweit die im Rahmen der Cloud-Nutzung gespeicherten Daten physisch nicht in den USA gespeichert werden, musste zunächst einmal ein Rückgriff auf den Foreign Intelligence

[28] Aufgrund Angemessenheitsbeschlusses der Europäischen Kommission vom 12.06.2016, abrufbar unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.
[29] *Datenschutzticker,* http://www.datenschutzticker.de/tag/eu-us-privacy-shield/.
[30] *Datenschutzbeauftragter,* https://www.datenschutzbeauftragter-info.de/praesident-trump-und-die-executive-order-das-aus-fuer-den-privacy-shield/; https://www.eaid-berlin.de/?p=1591.
[31] Ende März 2018 unterzeichnet, abrufbar unter https://www.congress.gov/bill/115th-congress/house-bill/4943/text.
[32] Vgl. *Landesbeauftragte für Datenschutz Freie Hansestadt Bremen,* 40. Jahresbericht zum Datenschutz, S. 89, abrufbar unter https://www.datenschutz.bremen.de/publikationen/jahresberichte-7242.
[33] *Landesbeauftragter für Datenschutz Freie Hansestadt Bremen,* 40. Jahresbericht, abrufbar unter https://www.datenschutz.bremen.de/publikationen/jahresberichte-7242.
[34] *Schwartz/Peifer,* CR 2017, 165, 165.
[35] *Schwartz/Peifer,* CR 2017, 165, 165.

Surveillance Act (FISA)[36], novelliert durch den (FISA Amendment Act) FAA 2008[37], ausscheiden.[38] Auch das Präsidialdekret Nr. 12333[39] hätte den US-Behörden nur dann eine Zugriffsmöglichkeit geboten, wenn die Nachrichtendienste das technische Knowhow gehabt hätten, die Daten in der deutschen Cloud zu entschlüsseln.[40] Zugang zu den auf den Cloud-Servern gespeicherten Daten wäre daher bisher am ehesten über den Stored Communication Act (SCA) als Bestandteil des Electronic Communications Privacy Act (ECPA) denkbar gewesen. Von besonderer Relevanz war hier die Auslegung der Eingriffsnorm des § 2703 United States Code (18 USC §§ 2701 et seq.)[41] durch die Gerichte. § 2703 USC erlaubt die Offenlegung von Kundenkommunikation und -unterlagen aufgrund einer richterlichen Durchsuchungsanordnung (Warrant).[42] Gleichzeitig blockiert er damit die Nutzung strafbewehrter Anordnungen (Subpoenas), die von den Behörden selbst erlassen, und (nur) von den Gerichten überprüft werden.[43] Die Auslegung der Eingriffsnorm und ihre Reichweite war allerdings lange umstritten.

3. Microsoft-Case

In dem sog. „Microsoft Ireland"-Fall galt es, Unklarheiten bzgl. der Eingriffsnorm zu ermitteln, welche Reichweite US-Durchsetzungsanordnungen hatten und ob sich diese auch auf außerhalb der USA gespeicherte Daten erstrecken konnten.[44] Das New Yorker Berufungsgericht hatte ein erstinstanzliches Urteil aufgehoben, wonach Microsoft der US-Regierung Zugriff auf E-Mail-Daten hätte geben müssen, welche auf irischen Servern (konkret in Dublin) gespeichert waren.[45] Die relevante Eingriffsnorm für die richterliche Dursuchungsanordnung war der oben angegebene § 2703 United States Code (USC) (18 USC §§ 2701 et seq.)[46].

---

[36] Foreign Intelligence Surveillance Act im Volltext abrufbar unter https://www.law.cornell.edu/uscode/text/50/chapter-36. Vgl. hierzu auch *Schwartz/Peifer,* CR 2017, 165, 168.
[37] Zu finden unter *Govtrack,* https://www.govtrack.us/congress/bills/110/hr6304.
[38] *Schwartz/Peifer,* CR 2017, 165, 173.
[39] Im Volltext abrufbar unter https://www.archives.gov/federal-register/codification/executive-order/12333.html.
[40] *Schwartz/Peifer,* CR 2017, 165, 168 und 173.
[41] Im Volltext abrufbar unter https://www.law.cornell.edu/uscode/text/18/2703.
[42] *Schwartz/Peifer,* CR 2017, 165, 167.
[43] *Schwartz/Peifer,* CR 2017, 165, 167.
[44] *Schwartz/Peifer,* CR 2017, 165, 165.
[45] Im Volltext abrufbar unter http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412. Hierzu auch *Schwartz/Peifer,* CR 2017, 165, 165.
[46] Im Volltext abrufbar unter https://www.law.cornell.edu/uscode/text/18/2703.

Das Berufungsgericht entschied, dass Microsoft die Daten nicht herausgeben müsse, nachdem die Norm nicht auf Fälle (Server) außerhalb der USA anwendbar sei. Dies wurde durch eine historische Auslegung des SCA begründet.[47] Hiernach sei nicht ersichtlich, dass der Kongress bei Erlass des SCA im Jahre 1986 Durchsuchungsanordnungen weltweite Geltung verschaffen wollte[48]. Bei Erlass des SCA sei eine internationale Vernetzung vielmehr noch unbekannt gewesen[49]:

„We conclude that Congress did not intend the SCA's warrant provisions to apply extraterritorially. The focus of those provisions is protection of a user's privacy interests. Accordingly, the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States."[50]

4. Änderungen im Zuge des CLOUD-Acts

Im Rahmen der Verabschiedung des CLOUD-Acts (Clarifying Lawful Overseas Use of Data Act) ist das Microsoft-Verfahren vor dem Supreme Court eingestellt worden, da nun eine Rechtsgrundlage für den in Streit stehenden Beschluss geschaffen wurde.[51]

Der neu geschaffene § 2713 (Chapter 121, title 18, United States Code (USC)) verpflichtet amerikanische Unternehmen unter bestimmten (durch den CLOUD-Act festgelegten) Voraussetzungen im Ausland gespeicherte und verarbeitete Daten, gleich wie im amerikanischen Inland gespeicherte Daten, vorzuhalten und bei entsprechenden Anfragen (durch amerikanische Behörden) preiszugeben. Maßgeblich ist hierbei zudem, dass die dort beschriebenen Verfahren eingehalten werden und schließlich, ob das betreffende Unternehmen die Kontrolle über die herauszugebenen Daten hat. Kontrolle beschreibt hierbei weder Eigentum oder Besitz sondern die Befugnis oder tatsächliche Möglichkeit, die Daten von einem Dritten zu verlangen.[52] Zwar wird den Unternehmen die Möglichkeit eingeräumt, die Preisgabe der entsprechenden Daten zu verhindern, etwa wenn es geltend machen kann, dass das Unternehmen mit der Preisgabe der Daten fremdes nationales Recht verletzen würde und betroffene Personen keine Bürger der USA sind und dort auch nicht

[47] *Schwartz/Peifer,* CR 2017, 165, 166.
[48] *Schwartz/Peifer,* CR 2017, 165, 166.
[49] *Schwartz/Peifer,* CR 2017, 165, 166.
[50] Case 14-2985, S. 42.
[51] *Gausling,* MMR 2018, 578, 579.
[52] Gem. Rul 34 und Rule 45 der Federal Rules of Procedure, vgl. *Determann/Nebel,* CR 2018, 408, 410.

ihren Wohnsitz haben (§ 2703 (h) (2) 18 USC). Die Stattgabe der Beschwerde ist allerdings auch dann nicht garantiert, denn die neu eingeführte Regelung fordert zusätzlich, dass Interessen der Rechtsvorgaben unter Berücksichtigung der Umstände die Stattgabe der Beschwerde gebieten (§ 2703 (h) (2) (B) 18 USC). Entsprechend der sog. Comity-Analyse (§ 2703 (h) (3) 18 USC) wird den Gerichten vorgegeben, welche Kriterien in die Interessenabwägung einzubeziehen sind. Als wichtiges Kriterium wird hierbei etwa das Untersuchungsinteresse der Vereinigten Staaten beschrieben. Es kann also nicht automatisch davon ausgegangen werden, dass amerikanische Gerichte den Herausgabeaufforderungen amerikanischer Behörden bei zu befürchtender Verletzung ausländischen Rechts immer eine Absage erteilen werden. Hinsichtlich eines Auftragsverhältnisses zwischen Deutschland und den USA kommt erschwerend hinzu, dass die Beschwerde gegen Auskunftsersuchen erst dann vorgebracht werden könnte, wenn aufgrund eines Executive Agreements zwischen Deutschland und den Vereinigten Staaten Deutschland als sog. qualifizierter Staat eingestuft wäre.[53] Ein solches scheint bisher nicht zu existieren.[54] Somit können amerikanische Cloud-Anbieter, nun sogar aufgrund ausdrücklicher Rechtsgrundlage, dazu gezwungen sein, Daten an amerikanische Behörden herauszugeben, auch wenn diese auf Servern in Deutschland gespeichert werden. Auf den zeitnahen Abschluss eines Exekutivabkommens ist daher nicht zuletzt aus Rechtssicherheitsgründen zu hoffen.[55]

5. Nutzerseitige Verschlüsselung oder Pseudonymisierung als Lösung?

Eine bereits nutzerseitige Verschlüsselung von Daten könnte dem Sicherheitsbedürfnis, wie es die DSGVO vorgibt, gerade bei grenzübergreifenden Sachverhalten im höheren Maße entsprechen. Eine solche könnte etwa als Teil technischer und organisatorischer Maßnahmen (TOM) im Sinne des Art. 32 Abs. 1 DSGVO umgesetzt werden. Der europäische Gesetzgeber stuft im Rahmen der TOM die Verschlüsselung, gleich wie die Pseudonymisierung von Daten, als besonders effektive Schutzmaßnahme ein, Art. 32 Abs. 1 a)

[53] *Gausling,* MMR 2018, 578, 580.
[54] Erst Ende 2018 ist in einem Treffen des Rates der Europäischen Union die Vereinbarung eines CLOUD-Act Abkommens mit den USA diskutiert worden und entsprechend eines EU-US Ministerial Treffens (November 8/9 2018) festgestellt worden, dass ein entsprechendes Abkommen vorzugsweise zwischen den USA und der EU und nicht zwischen den USA und einzelnen Mitgliedsstaaten vereinbart werden sollte, vgl. *Council oft he European Union,* Pressemitteilung 15252/18 PUBLIC, S. 17.
[55] Vgl. auch *Determann/Nebel,* CR 2018, 408, 412.

DSGVO.[56] Auch das ULD Schleswig Holstein geht davon aus, dass im Einzelfall einigen gerügten Datenschutzmängeln von Microsoft-Produkten über eine hinreichende Verschlüsselung und Pseudonymisierung begegnet werden kann.[57] Mit der hier vertretenen Auffassung würde eine bereits nutzerseitige Verschlüsselung über die Datensicherheit hinaus auch die Datenhoheit des Verantwortlichen festigen, die Qualifizierung des Cloud-Anbieters als Auftragsverarbeiter im Sinn des Art. 28 DSGVO wäre demzufolge unproblematischer. Ein Zugriff amerikanischer Behörden auf diese Daten würde durch die Verschlüsselung zumindest erschwert. Der Einsatz einer Verschlüsselung ist indes nur dann sinnvoll, wenn diese tatsächlich in der Lage ist, einen unautorisierten Zugriff des Cloud-Anbieters auf die Daten des Auftraggebers auch faktisch zu unterbinden. Das Konzept der Verschlüsselung wird von der Datenschutzgrundverordnung zwar nicht ausdrücklich definiert[58], Art. 34 Abs. 3 a) DSGVO beschreibt sie jedoch als insbesondere solche technischen und organisatorischen Vorkehrungen, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den Daten befugt sind, unzugänglich gemacht werden. Eine Verschlüsselung kann sowohl mit Betriebssystemen als auch software- oder hardwareunterstützt stattfinden.[59] Im Rahmen der Verschlüsselung (engl. Encryption) kommen sowohl symmetrische als auch asymmetrische Verfahren in Betracht.[60] Welche Verschlüsselungsvariante gewählt wird, ist individuell den Bedürfnissen und infrastrukturellen Möglichkeiten des Verantwortlichen anzupassen. Beispielhaft soll hier nur der Advanced Encryption Standard (AES) als moderne symmetrische Verschlüsselungsvariante beschrieben werden. Der AES kann deswegen als sehr sicher beschrieben werden, weil aufgrund besonders langer Schlüssellänge eine vollständige Schlüsselsuche zu aufwendig wäre. Dies gilt selbst für Brute Force Attacken.[61] Über einige theoretische An-

[56] Vgl. *Voigt,* IT-Sicherheitsrecht, 2018, S. 129.
[57] *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, abrufbar unter https://www.datenschutzzentrum.de/tb/tb35/kap07.html.
[58] Vgl. hierzu auch *Hansen,* in: Simitris/Hornung/Spiecker, Datenschutzrecht, DSGVO Art. 32, Rn. 35.
[59] Für weitere Informationen, vgl. *BSI,* Datenverschlüsselung, https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Datenverschluesselung/datenverschluesselung_node.html.
[60] Im Falle der symmetrischen Verschlüsselung wird für die Verschlüsselung als auch Entschlüsselung der gleiche Schlüssel eingesetzt, beim asymmetrischen Verfahren wird mit unterschiedlichen Schlüsseln operiert, mehr hierzu vgl. *Reiner Kraft et. al.,* Vertraulichkeitsschutz durch Verschlüsselung, 03/2015, S. 13 ff, abrufbar unter https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Vertraulichkeitsschutz_durch_Verschluesselung.pdf?_=1442501295.
[61] *Luber,* security-insider, https://www.security-insider.de/was-ist-aes-advanced-encryption-standard-a-688378/; bei Brute Force Attacken wird durch automatisiertes Ausprobieren versucht, Passwörter oder

griffsvarianten hinaus sind keine ernsthaften, bzw. praktikablen Schwächen des AES bekannt.[62] Seit der Einführung der Advanced Encryption sind darüber hinaus zahlreiche weitere symmetrische Verfahren wie MISTY1, KASUMI und ähnliche geschaffen worden. Auch sie können einen hohen Standard bieten.[63] Hier obliegt es dem Verantwortlichen, sich zu informieren oder beraten zu lassen, welche Verschlüsselungsverfahren für seine Bedarfe und infrastrukturellen Möglichkeiten praktikabel und wirksam sind.

Wie eingangs erwähnt, benennt die Datenschutzgrundverordnung neben der Verschlüsselung im Übrigen auch die Pseudonymisierung von Daten als Methode, um den unbefugten Zugang Dritter zu personenbezogenen Daten zu unterbinden. Es ist jedoch fraglich, ob Pseudonymisierung im vorliegenden Kontext überhaupt als wirksame Methode eingesetzt werden kann: So wird bereits in Frage gestellt, ob Anonymisierung angesichts künftiger Nutzung von Quantencomputing und der diesem innewohnenden Rechenkraft in vernetzten Systemen unerwünschte Zugriffe auf (ehemaligen bzw. verborgenen) personenbezogene Daten wirksam unterbinden kann. Um so mehr muss gefragt werden, ob die Vergabe von Pseudonymen einen durchgreifenden Schutz bietet, wo doch umgekehrt die Verwaltungspraxis im Gesetzesvollzug auf die Verarbeitung der personenbezogenen Daten angewiesen ist. Allemal bleibt die Herausforderung, die Vergleichsdatenbank zur Auflösung der Pseudonyme im Wirkbetrieb ausreichend zu schützen.

IV. Erhebung und Versendung von Telemetriedaten bei MS Office 365

Im Rahmen von Neuüberlegungen bzgl. der datenschutzrechtlichen Konformität von US-Clouds und der DSGVO, insbesondere in öffentlichen Einrichtungen, ist die Erhebung von sog. Telemetriedaten in den Vordergrund gerückt. Telemetriedaten sind diejenigen Daten, die im Zusammenhang mit der Nutzung von IT-Produkten erhoben werden und Aussage über dessen Funktionsweise geben. Die vom niederländischen Justizministerium in Auftrag gegebene Studie beurteilte den Einsatz von Office 365 ursprünglich kritisch und hielt insbesondere die (bis dato) intransparente Erhebung von Telemetriedaten für einen Verstoß gegen die Vorgaben der DSGVO.[64] Die Ersteller der Studie sahen in der konkreten

Schlüssel zu ermitteln, *Luber/Schmidt,* security-insider, https://www.security-insider.de/was-ist-ein-brute-force-angriff-a-677192/.

[62] Vgl. auch zu den Grundlagen der Verschlüsselung, *Schmeh,* Kryptografie: Verfahren, Protokolle, Infrastrukturen, 2016, 10.3.

[63] *Schmeh,* Kryptografie: Verfahren, Protokolle, Infrastrukturen, 2016, 12.1. ff.

[64] Microsoft Office Pro Plus Studie, vgl. Fn. 7.

Ausgestaltung von Microsoft Office Verstöße gegen das Zweckbindungsgebot, das Transparenzerfordernis sowie die Rechtmäßigkeit der Datenverarbeitung. Auch wurde die nicht auszuschließende Versendung der Telemetriedaten (Diagnosedaten) an außereuropäische Standorte bemängelt. Soweit ausdrückliche Regelungen zum Speicher- und Versandort von Daten nur hinsichtlich der Kerndaten (etwa vom Nutzer gewollt in der Cloud gespeicherte Daten) existieren und Telemetriedaten nicht Gegenstand dieser Regelung werden, verstößt die Versendung in Drittländer gegen die Bestimmungen der DSGVO.[65] Auf die CLOUD-Act-Problematik geht die Studie im Übrigen nicht näher ein[66]. Zwar konnte bereits zum Studienzeitpunkt in den Einstellungen das Ausmaß der Diagnosedatenerhebung eingeschränkt werden, eine vollständige Abschaltung war indes nicht möglich. Im Rahmen der datenschutzrechtlichen Beurteilung wird davon ausgegangen, dass auch die erhobenen Diagnosedaten personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO darstellen können.[67] Mangels weiterer Informationen hinsichtlich der Diagnosedaten seitens des Betreibers von Microsoft Office konnten genauere Angaben (etwa über die Art und Weise und konkret welche Diagnosedaten erhoben wurden), nicht gemacht werden, daher auch der Transparenz-Vorwurf.[68] Bisher wurden die Diagnosedaten seitens Microsoft nicht als gesonderte Daten behandelt, und vertraglich im Zusammenhang mit sämtlichen erhobenen Daten zusammengefasst. Für einige Office-Produkte sind seitens Microsoft seither allerdings Änderungen hinsichtlich der Möglichkeiten, die Erhebung von Diagnosedaten zu unterbinden, eingeführt worden.[69] So soll es bei Office 365 ProPlus mittlerweile möglich sein, die Erhebung und Versendung von Diagnosedaten vollständig auszuschalten.[70] Der hessische Datenschutzbeauftragte sieht dessen Einsatz in Schulen aufgrund einer jüngsten Einschätzung daher auch weniger problematisch als bisher.[71] Auch dem Transparenzvorwurf wurde bereits begegnet, indem weitreichend Informationen bzgl. erhobener Diagnosedaten bereitgestellt werden.[72]

---

[65] Microsoft Office Pro Plus Studie, vgl. Fn. 7, Seite 52 und 53.
[66] Vgl. aber Microsoft Office Pro Plus Studie, vgl. Fn. 7, Seite 82.
[67] Microsoft Office Pro Plus Studie, vgl. Fn. 7, Seite 16; *Gerlach* CR 2020, 165, 166
[68] Vgl. auch *Gerlach* CR 2020, 165, 166 f.
[69] *Microsoft,* Übersicht über Datenschutzkontrollen für Office 365 ProPlus, https://docs.microsoft.com/de-de/deployoffice/privacy/overview-privacy-controls.
[70] *Microsoft,* Übersicht über Datenschutzkontrollen für Office 365 ProPlus, https://docs.microsoft.com/de-de/deployoffice/privacy/overview-privacy-controls.
[71] *Hessischer Beauftragter für Datenschutz und Informationsfreiheit,* Zweite Stellungnahme zum Einsatz von Microsoft Office 365, https://datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen.
[72] Vgl. hierzu mitunter: *Microsoft,* Für Office erforderliche Diagnosedaten, https://docs.microsoft.com/de-de/deployoffice/privacy/required-diagnostic-data.

Im Einzelnen sehen die Studienersteller bereits die Rechtsgrundlage der Datenverarbeitung nicht gegeben, mit der Begründung, dass regelmäßig eine Einwilligung fehle, weil Telemetriedaten nicht zum Gegenstand der Vertragswerke werden. Gerade die Einwilligung von Behördenmitarbeitern (gleiches wird regelmäßig für Arbeitnehmer gelten) fehle meist.[73] Dass die Datenerhebung zu Zwecken der Vertragserfüllung zwingend erforderlich und somit rechtmäßig sein könne, bezweifeln die Autoren zumindest hinsichtlich eines Teils dieser Diagnosedaten.[74] Dass etwa Nutzer nachträglich den Umfang der erhobenen Telemetriedaten einschränken könnten, zeige dass die Vertragserfüllung nicht zwingend die Erhebung sämtlicher der ursprünglich voreingestellten Telemetriedaten erfordere. Umgekehrt kann hieraus der Schluss gezogen werden, dass über die zwingend erforderlichen Telemetrie- und Diagnosedaten hinaus erhobene Daten nicht als Opt-Out, sondern als Opt-In Funktion ausgestaltet werden sollten.

Im Rahmen der Einordnung des Cloud-Nutzers und des Cloud-Anbieters ist darüber hinaus nicht ausreichend geklärt, wer für die Daten verantwortlich im Sinne der DSGVO ist. Den Cloud-Nutzer (z.B. ein Unternehmen) als Verantwortlichen anzusehen, ist insofern problematisch, als er Art und Maß der Datenerhebung kaum beeinflusst und auch nicht ausreichend transparent über die Erhebung von Telemetriedaten informiert ist. Eine vorgezogene Weisung kann mithin nicht automatisch unterstellt werden. Dies macht jedoch das Finden einer Rechtsgrundlage für die Datenerhebung umso schwieriger, denn z.B. Arbeitnehmer sind überwiegend nicht Vertragspartner des Cloud-Nutzungs-Vertrags.[75] Gleichwohl ist festzustellen, dass Microsoft sich mit dem Bedenken der Studie auseinandersetzt und über die adressierten Themen mit dem niederländischen Justizministerium verhandelt hat. [76]

---

[73] Microsoft Office Pro Plus Studie, vgl. Fn. 7, Seite 63.

[74] Microsoft Office Pro Plus Studie, vgl. Fn. 7, Seite 64f.; grundsätzlich verneinend für die Offenlegung von Telemetriedaten *Gerlach* CR 2020, 165, 169

[75] Vgl. hierzu ebenfalls Microsoft Office Pro Plus Studie, vgl. Fn. 7, Seite 62; *Gerlach* CR 2020, 165, 169

[76] Microsoft hat zum 08.01.2020 seine Online Service Terms (OST) für kommerzielle Kunden entsprechend den Verhandlungen mit dem niederländischen Justizministerium angepasst und dabei eingeräumt, dass es Verantwortlicher in Hinblick auf „Datenverarbeitung [zu] administrativen oder operativen Zwecken, wie etwa der Kontoführung, Finanzberichterstattung, Bekämpfung von Cyberangriffen auf Microsoft-Produkte oder -Dienstleistungen sowie Erfüllung unserer gesetzlichen Verpflichtungen“ ist. Es wird jedoch auch noch einmal hervorgehoben, dass Microsoft „Auftragsverarbeiter für die Bereitstellung der Dienste, die Ausbesserung und Behebung von Fehlern oder anderen Problemen im Zusammenhang mit einem Dienst, die Gewährleistung der Sicherheit der Dienste und die Aktualisierung der Dienste“ bleibt. Somit ändert sich an den Ausführungen im Ergebnis nichts. Ankündigung der Änderung der OST: https://news.microsoft.com/de-de/einfuehrung-von-mehr-datenschutztransparenz-fuer-unsere-kommerziellen-cloud-kunden/; Mitteilung, dass die OST nun zur Verfügung stehen: https://news.microsoft.com/de-de/update-microsoft-online-services-terms/.

Im Übrigen setzt sich die Studie auch kurz mit Cloud-Angeboten anderer Dienstleister auseinander. Keine dieser Produkte, so die Autoren, stelle eine datenschutzrechtlich bessere Alternative dar.[77] Im Ergebnis gilt für diese anderen Cloud-Angebote die gleiche Risikobeurteilung. Microsoft hat nach eigenen Angaben bereits reagiert und eine Einschränkung des Versands von Telemetriedaten in einer Vielzahl von Office 365 Produkten ermöglicht.

V. Erhebung und Versendung von Telemetriedaten bei MS Windows 10

Neben einer direkten und klassischen Cloud-Nutzung durch Unternehmen oder öffentliche Behörden, bei welcher vom Anwender bestimmte Daten in eine Cloud geladen werden, sind auch Modelle, bei denen Betriebsfunktionen unter Nutzung der Cloud-Vorteile zur Verfügung gestellt werden, nicht minder datenschutzrechtlich relevant. Das Betriebssystem von Microsoft, Windows 10, stellt ein solches System dar. Dieses aktuelle Betriebssystem von Microsoft soll unter anderem mit automatisch über eine Cloud abrufbaren Updates für eine erhöhte IT-Sicherheit sorgen.[78] Die Cloud-Zentrierung des neuen Betriebssystems wird allerdings hinsichtlich Datenschutz und Sicherheit kritisiert.[79] Im Rahmen der Windows 10-Nutzung werden ebenfalls regelmäßig Telemetriedaten abgefragt, unter anderem über die Rechnerverwendung, aufgerufene URLs, WLAN-Schlüssel, User-IDs, etc.[80] Es stellen sich hier im Wesentlichen die gleichen Fragen wie bei der Erhebung von Telemetriedaten im Rahmen der klassischen Cloud-Nutzung durch den Endanwender, so auch bei Microsoft Office 365. Für den datenschutzrechtlich Verantwortlichen stellt sich die Einhaltung der DSGVO-Vorgaben nach Ansicht der Datenschutzkonferenz als mindestens erheblich aufwendig dar. Sie fordert daher die Einräumung der technischen Möglichkeit, sämtliche Datenübermittlungen zu unterbinden.[81] Bereits 2017 wurde Windows 10 in einer koordinierten Aktion der Datenschutzaufsichtsbehörden u.a. aus Deutschland, Frankreich und den Niederlanden hinsichtlich der Datenschutzkonformität

[77] Microsoft Office Pro Plus Studie, vgl. Fn. 7, Seite 72.
[78] Vgl. hierzu *Kranawetter,* Kes – die Zeitschrift für Informations-Sicherheit, 2019, Ausgabe 1, 16, 19.
[79] Vgl. *Grundwald,* Report „Datenschleuder – Welche Informationen Windows 10 in die Cloud übermittelt", abrufbar unter https://www.heise.de/select/ix/2016/11/1478346039425819.
[80] Vgl. hierzu sowohl *Kranawetter,* Kes – die Zeitschrift für Informations-Sicherheit, 2019, Ausgabe 1, 16ff, als auch *Grundwald,* Report „Datenschleuder – Welche Informationen Windows 10 in die Cloud übermittelt", abrufbar unter https://www.heise.de/select/ix/2016/11/1478346039425819.
[81] *Datenschutzkonferenz,* Auftrag der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Positionierung der DSK zum datenschutzkonformen Einsatz von Windows X.

geprüft. Die Behörden kamen hierbei zu dem Schluss, dass ein Einsatz des Betriebssystems zulässig sei, insofern die Möglichkeit besteht, die Übersendung von Telemetriedaten zu unterbinden.[82] Dies bedeutet jedoch auch, dass die Standardinstallation des Betriebssystems zu Beginn der Nutzung nicht die datenschutzfreundlichsten Voreinstellungen hat, sondern ein aktives Abschalten durch den Anwender erfordert. Art. 25 Abs. 2 DSGVO verpflichtet jedoch den Verantwortlichen zu „Privacy by Default", also der Schaffung von Voreinstellungen mit dem höchsten Datenschutz.[83] Um festzustellen, ob das Prinzip des Privacy by Default durch Windows 10 verletzt wird, ist eine Einzelfallprüfung durchzuführen. Wird Windows 10 genutzt, so müssen Maßnahmen getroffen werden, um eine unzulässige Offenlegung von personenbezogenen Daten zu verhindern. Die Auswahl und Angemessenheit dieser Maßnahmen hängen von den Implementierungskosten, den Risiken für die Rechte der betroffenen Personen sowie dem Stand der Technik ab. Verbleibt auch nach Durchführung dieser Maßnahmen ein Restrisiko, so ist zu bewerten, ob dieses Restrisiko tragbar ist.

Windows 10 bietet die Auswahl zwischen verschiedenen Editionen des Betriebssystems, die der Nutzer je nach Wünschen und Anforderungen wählen kann. So kann beispielsweise zwischen der Home-Edition, der Pro-Edition, der Enterprise-Edition usw gewählt werden. Diese Editionen unterscheiden sich durch die Services, die durch Windows 10 in der jeweiligen Edition zur Verfügung gestellt werden. So bietet die Enterprise-Edition (im Gegensatz zur Pro-Edition) beispielsweise größere Sicherheiten für den Nutzer, da diese Edition des Betriebssystems Microsoft Defender Advanced Threat Protection (ATP) enthält, das vor Cyberbedrohungen schützt und Angriffe und Datenschutzverletzungen erkennt, wodurch die Sicherheit gestärkt wird. Für den Nutzer von Windows 10 besteht die Möglichkeit, die Einstellungen an der Konfiguration so vorzunehmen, dass er diese seinen individuellen Wünschen anpassen kann. Der Umfang dieser Einstellungsmöglichkeiten unterscheidet sich je nach gewählter Edition des Betriebssystems. So besteht beispielsweise bei der Enterprise-Edition auch eine umfangreichere Einstellmöglichkeit als bei der Home-Edition.

Zu beachten bleibt, dass jedes durchgeführte Update zur Folge haben kann, dass die Konfigurationseinstellungen geändert werden, was wiederum dazu führen kann, dass ein

[82] ZD-Aktuell 2017, 05774.
[83] Vgl. hierzu auch *Kühling/Buchner,* DSGVO – BDSG, DSGVO Art. 25, Rn. 24 ff.

„neues Produkt“ vorliegt und demzufolge die datenschutzrechtliche Zulässigkeit nach Durchführung eines solchen Updates erneut seitens des Verantwortlichen geprüft werden muss.[84]

Bevor der Einklang mit der DSGVO nicht gewährleistet werden kann, muss ein Wechsel des Betriebssystems vorsichtig durchgeführt werden, da je nach Konfiguration durch Windows 10 (und etwaige Zusatzfunktionen) Daten zwischen dem betroffenen Computer und Microsoft ausgetauscht werden könnten.

Die Problematik verschärft sich durch die Versendung von Telemetriedaten in Drittstaaten, ohne dass schon zu Beginn der Datenerhebung eine Prüfung durch den Anwender möglich ist. Der Auffassung der Behörden muss daher entnommen werden, dass das Betriebssystem Windows 10 zwar nicht per se datenschutzkonform ist, dessen datenschutzkonformer Einsatz allerdings hergestellt werden kann. Welche Daten im Einzelnen wiederum von einer Rechtsgrundlage der DSGVO gedeckt sind[85] (in Betracht kommt hier überwiegend etwa die Erforderlichkeit zur Vertragserfüllung, Art. 6 Abs. 1 b) DSGVO, bei Beschäftigtendaten ggf. auch § 26 BDSG), hängt von den konkret erhobenen Daten und deren Verwendungszweck ab.

Werden personenbezogene Daten erhoben und erfolgt die Übermittlung dieser Daten an Server in den USA, führt dies dazu, dass die Regelungen der Art. 44 ff. DSGVO anwendbar sind. Bei Microsoft handelt es sich um ein nach dem Privacy Shield zertifiziertes Unternehmen. Dies bedeutet, dass Microsoft sich zur Einhaltung der Grundsätze des Privacy Shield verpflichtet hat und auf der Website des US Department of Commerce gelistet ist. Gestützt auf das Privacy Shield hat die EU-Kommission beschlossen, dass die Übermittlung von personenbezogenen Daten in die USA zulässig ist, sofern die genannten Voraussetzungen erfüllt sind. Soweit die Geltung des Angemessenheitsbeschlusses der Kommission sowie die Einhaltung der Privacy Shield Standards durch Microsoft aufrechterhalten und beibehalten werden, erlaubt die DSGVO also grundsätzlich die Datenübermittlung.

[84] Auftrag der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Positionierung der DSK zum datenschutzkonformen Einsatz von Windows 10, S. 1.
[85] Vgl. hierzu bereits oben S. 15.

VI. Technisch-organisatorischer Datenschutz

Nach Art. 25 DSGVO ist der Verantwortliche dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um den datenschutzrechtlichen Grundsätzen Gewähr zu leisten. Art. 25 DSGVO ist nicht an den Hersteller, sondern vielmehr an den Verantwortlichen adressiert, weshalb ihm diese (Schutz-)Pflicht zukommt und er somit den Datenschutz durch entsprechende Technikgestaltung zu wahren hat. Hierbei steht auch das Transparenz- und Vertraulichkeitsgebot im Vordergrund. Den Verantwortlichen trifft die Pflicht zum Nachweis der Einhaltung dieser Grundsätze. Er hat von den auf dem Markt verfügbaren Betriebssystemen und Cloud-Angeboten jenes auszuwählen, das diesen Grundsätzen am ehesten entspricht und den Datenschutz bestmöglich einhält. Art. 5 Abs. 1 c) DSGVO normiert des Weiteren den Grundsatz der Datenminimierung, der die Verpflichtung beinhaltet, die Verwendung personenbezogener Daten nur zweckgemäß zu gestalten und auf das notwendige Maß zu beschränken. Wie bereits dargestellt, besteht beim Einsatz von Windows 10 und Office 365 das Risiko, dass als Teil der Telemetriedaten auch personenbezogene Daten an Microsoft übermittelt werden. Diesem Risiko muss mit entsprechend geeigneten technisch-organisatorischen Maßnahmen im Sinne des Art. 25 Abs. 2 DSGVO entgegengewirkt werden, um den Anforderungen der DSGVO zu genügen. Es bleibt im Einzelfall zu prüfen, welche Maßnahmen in concreto als geeignet anzusehen sind. Dabei sind sowohl die Eintrittswahrscheinlichkeit als auch die Schwere des Risikos zu beurteilen. Insbesondere die Schwere des Risikos hängt von diversen Faktoren ab, wie beispielsweise von dem von Microsoft verfolgten Zweck sowie der Art der jeweils verarbeiteten Daten und deren Umfang.

Wie bereits oben ausgeführt, ist z.B. bei der Standardinstallation von Windows 10 nicht die datenschutzfreundlichste Voreinstellung gegeben; daher muss die Datenschutzkonformität durch den Verantwortlichen herbeigeführt werden. Da die mögliche Übermittlung von Daten an Microsoft bei den meisten Versionen nicht vollständig unterbunden werden kann, sind weitere technische Maßnahmen zu treffen, um diese Übermittlung zu beschränken bzw. zu kontrollieren. Die Enterprise Version von Windows 10 lässt zumindest eine so weitgehende Beschränkung der Erhebung von Diagnosedaten zu, dass nur

diejenigen Daten erhoben werden, die erforderlich sind, um Windows-Geräte und -Server mit den neusten Sicherheitsupdates zu schützen.[86]

Da sich der Verordnungsgeber (bewusst) gegen eine Herstellerverantwortlichkeit entschieden hat, kann der Hersteller gegenüber dem Verantwortlichen nicht dazu angehalten werden, die datenschutzfreundlichsten Voreinstellungen zu wählen. Daher liegt es am Verantwortlichen (also der Behörde/dem Unternehmen etc.), der sich für den Einsatz von Cloud-Produkten US-amerikanischer Anbieter entschieden hat, eine Konfiguration vorzunehmen, die nur die notwendigen und zweckmäßigen Daten verarbeitet.

Von einer vollständig fehlenden Transparenz hinsichtlich der Telemetriedatenübermittlung kann indes nicht mehr ausgegangen werden. Microsoft stellt etwa im Rahmen von Windows 10 ein Werkzeug zur Verfügung, mit dem Einblicke über die übermittelten Telemetriedaten gegeben werden.[87] Diese App, genannt „Diagnostic Data Viewer", lässt den Nutzer die Diagnosedaten überprüfen, die vom genutzten Gerät an Microsoft gesendet werden.[88] Sollen im Rahmen der Windows 10-Benutzung möglichst wenig Telemetrie-, bzw. Diagnosedate preisgegeben werden, so ist es zumindest möglich, den Umfang festzulegen und zu begrenzen.[89] Mit Hilfe dieser App ist es nicht nur möglich, den Umfang der Erhebung einzugrenzen bzw. einzusehen welche Daten übermittelt werden, sondern auch bereits erhobene Diagnosedaten zu löschen. Derzeit ist es jedoch auch trotz dieser App nicht möglich, die Datenübertragung an Microsoft, außerhalb der Enterprise Version, auf das für die Betriebssicherheit relevante absolute Minimum zu beschränken; außerdem ist durch die Verschlüsselung der Daten schwer nachvollziehbar, ob bzw. welche personenbezogenen Daten übermittelt werden.
Zu beachten ist auch, dass die innerhalb des Betriebssystems Windows 10 erhobenen Telemetriedaten vielfach keine personenbezogenen Daten sind. Vielmehr geht es darum, Aufschluss darüber, welche Websites oder Apps Probleme bereiten, über Fehlfunktionen des Arbeitsspeichers, den Stand von möglichen Updates, die Analyse von Fehlermeldungen etc. geben zu können. Zum Schutz der personenbezogenen Daten werden gesonderte

[86] Siehe hierzu *Microsoft,* Konfigurieren von Windows-Diagnosedaten in Ihrer Organisation, https://docs.microsoft.com/de-de/windows/privacy/configure-windows-diagnostic-data-in-your-organization.
[87] *Mahn,* heise, https://www.heise.de/newsticker/meldung/Windows-10-Telemetrie-Daten-An-Microsoft-geschickte-Infos-ueberwachen-3950591.html.
[88] *Microsoft,* Übersicht über den Diagnostic Data Viewer, https://docs.microsoft.com/de-de/windows/privacy/diagnostic-data-viewer-overview.
[89] *Kranawetter,* Kes – die Zeitschrift für Informations-Sicherheit, 2019, Ausgabe 1, 16, 19.

Server verwendet, die erkennbare persönliche Daten automatisch entfernen oder maskieren. Dies wird beispielsweise durchgeführt, wenn solche Daten zufällig in Systemprotokollen o.Ä. enthalten sind.[90] Telemetriedaten können jedoch unter Umständen auch personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO enthalten, wie beispielsweise beim Memory Dump. Beim Memory Dump (Speicherabbild) handelt es sich um einen Vorgang, bei dem der Speicherinhalt angezeigt und bei einem Systemabsturz gespeichert wird. Somit leistet das Speicherabbild Hilfestellung bei der Identifizierung und Behebung des Problems, das für den Systemausfall ursächlich war. Das Speicherabbild liefert Informationen über den letzten Zustand der Systeme, Programme und Anwendungen, bevor diese beendet wurden bzw. abgestürzt sind. Solche Informationen können beispielsweise Programmstatus, Programmzähler, Speicherplätze etc. beinhalten.[91] Durch diese erhobenen Telemetriedaten kann geprüft werden, wie viele Geräte von Fehlermeldungen betroffen sind, ob es sich um eine Fehlermeldung von einem einzigen Gerät handelt oder um tausende Fehlermeldungen von tausenden Geräten. Schwachstellen und Fehler sind umso leichter zu ermitteln, je mehr Diagnosedaten erhoben und übermittelt werden. Dadurch soll gewährleistet werden, dass etwaige Fehler durch Microsoft leichter und schneller behoben werden.

Zusammengefasst zielt die Erhebung von Telemetriedaten im Rahmen von Windows 10 und Office 365 darauf ab, die Zuverlässigkeit, Stabilität und Sicherheit von IT-Systemen zu gewährleisten und zu verbessern. Bei der Verwendung der Produkte ist bis dato in Hinblick auf die datenschutzrechtliche Konformität Vorsicht geboten. Bei der Enterprise Version von Windows 10 sowie Office 365 ProPlus kann jedoch durch die Einstellungs- und Überwachungsmöglichkeiten seitens des Nutzers ein datenschutzkonformer Einsatz im Sinne der DSGVO möglich sein.

Dieses Ergebnis bestätigt auch Vitako e.V., mit Verweis auf einen Brief des niederländischen Innenministers und Justizministers an das Parlament[92]: „Aus [diesem Brief] geht nun hervor, dass die Änderungen, die der Software-Hersteller an seinen Produkten vorgenommen hat, in Ordnung seien. Außerdem haben sich die Niederlande mit Microsoft auf zusätzliche Datenschutzvorkehrungen geeinigt, die nun den Einsatz von Windows 10

[90] *Kranawetter*, Kes – die Zeitschrift für Informationssicherheit, 2019, Ausgabe 1, Seite 18.
[91] *Techopedia,* Memory Dump, https://www.techopedia.com/definition/20663/memory-dump.
[92] *VITAKO,* https://206182.seu2.cleverreach.com/m/11492257/560141-c8a550f41b055209828ab4b36b129677.

und Office 365 ProPlus unter Einhaltung der DSGVO ermöglichen sollen. Unter anderem wird klar festgelegt, zu welchen Zwecken Daten verarbeitet werden dürfen und dass die Weitergabe an Dritte ausgeschlossen ist. Auch neue Datenschutzfolgeabschätzungen sehen nun keine hohen Risiken mehr in den Telemetrie-Daten bei Windows 10 und Office 365 ProPlus. Hierbei muss allerdings beachtet werden, dass hier ausschließlich die Erfassung und Übermittlung von Telemetrie-Daten betrachtet wird und auch dabei noch keine Entwarnung bei Office 365 Online und den Office-365-Mobil-Apps gegeben wurde. Das Speichern von Daten in der Cloud war nicht Teil der Untersuchung. Für den Fall, dass Daten doch nicht in lokalen Rechenzentren gespeichert werden, wird empfohlen, diese nur verschlüsselt in der Microsoft-Cloud abzulegen.[93]

VII. Fazit

Im Ergebnis dürfte für die Nutzung von Clouddiensten amerikanischer Anbieter festzustellen sein, dass die Angemessenheit des Datenschutzniveaus in den USA immer noch kritisch zu beurteilen ist, gleichwohl Unsicherheiten weiträumig durch eine Zertifizierung der Cloud Anbieter unter dem Privacy Shield oder den Abschluss der sog. EU-Standardvertragsklauseln kompensiert werden. Festzustellen ist jedoch auch, dass andere am Markt verfügbare Cloud-Angebote entweder (wie Google Cloud) ebenfalls nicht frei von datenschutzrechtlichen Bedenken sind oder kein mit den Office-Lösungen in Microsoft 365 vergleichbares Portfolio bieten.

Für die Gewährleistung eines effektiven Datenschutzes bedarf es der engen Zusammenarbeit zwischen Auftraggeber und potenziellem Auftragnehmer. Microsoft etwa hat bereits den Willen zu erkennen gegeben, an der Datenschutzkonformität angebotener Cloud-Modelle zu arbeiten.[94] Ein Unternehmen oder eine Behörde, die Modelle wie die Microsoft Cloud Deutschland in Anspruch nehmen möchte, sollte sich dessen und seines Haftungsrisikos aufgrund der Position als datenschutzrechtlich Verantwortlicher bewusst sein. Eine wirksame nutzerseitige Verschlüsselung etwa kann den geforderten Sicherheitsstandard erhöhen. Eine Herausgabe der Daten durch den amerikanischen Cloud-Anbieter ist letztlich aber nicht auszuschließen. Zu beachten ist, dass die DSGVO mit ihrem

[93] Vgl. auch https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise.

[94] Siehe hierzu *Reimann,* Datenschutz bei Microsoft: Kontrolle, Transparenz und Sicherheit für Kunden weltweit, https://news.microsoft.com/de-de/datenschutz-microsoft/.

risikoadaptierten Ansatz keine „100%-ige Sicherheit“ fordert, auch nicht bei solchen Anbietern, die sich nicht im Anwendungsbereich der DSGVO befinden.[95] Datenschutz ist ein hohes Gut, steht aber zuweilen in Konflikt mit anderen Werten oder legitimen Interessen. So fordert auch Art. 25 Abs. 1 DSGVO technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten „unter Berücksichtigung des Stands der Technik der Implementierungskosten ... sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken“. Kurz gesagt: Datenschutz nicht um jeden Preis. Besonderes Augenmerk sollte gleichwohl auf die konkrete Ausgestaltung des Cloud-Angebots, der Wahrung von Transparenz und zumindest soweit wie möglichen Unterbindung des Zugriffs Dritter auf diese Daten gelegt werden. Was wiederum die Nutzung spezieller Anwendungen wie Microsoft Office 365 oder Microsoft Windows 10 betrifft, ist zu überlegen, ob der risikobasierte Ansatz[96] der DSGVO in Anbetracht der hohen Migrationskosten bei der Suche nach Alternativen für die Bürokommunikation der Behörden nicht auch eine vorübergehende Inkaufnahme von Datenschutzrisiken zulässt. Insofern wäre eine Abwägung zu treffen zwischen den Interessen der datenschutzrechtlich Betroffenen und dem behördlichen Interesse an einer wirtschaftlich-organisatorisch angemessenen Erledigung öffentlicher Aufgaben. Dies bedeutet aber auf keinen Fall einen Freifahrtschein für den Verantwortlichen zum "Nichtstun." Und ebenso ist Microsoft gehalten, zur Risikominimierung beizutragen.

Im Rahmen der Abwägung ist auch zu berücksichtigen, dass sich die Datenschutzkonferenz auch nach jahrelanger Befassung noch nicht zu einem klaren Votum durchgerungen hat. Daraus ergibt sich eine Rechtsunsicherheit, die weder zu Lasten der Anwender noch der schützenswerten Daten der Bürger gehen darf. Man kann auch pointiert von einer „konzertierten Nicht-Aktion“ der Datenschutzaufsicht sprechen, aus der man eine zumindest vorübergehende Duldung der Nutzung der genannten Cloud-Angebote ableiten kann. Das befreit die Nutzer nicht davon, Alternativen zu suchen, zu beurteilen und im Hinblick auf die Vorteile und Nachteile einer Migration zu gewichten. Dabei sind insbesondere die berechtigten Schutzinteressen Dritter zu beachten. Die getroffene Entscheidung ist zu be-

[95] Daran ändert die Alternative „Open Source“ auch nichts, wie das „Hin und her“ der Stadt München im. Projekt „Limux“ zeigt, hierzu jüngst https://www.golem.de/news/limux-muenchen-will-wieder-open-source-software-praeferieren-2005-148303.html.

[96] Hierzu ausdrücklich auch das im Oktober 2019 vorgelegte Gutachten der Datenethikkommission, www.datenethikkommission.de.

gründen und zu dokumentieren. Stellungnahmen der zuständigen (Landes-) Datenschutzaufsicht und der Datenschutzkonferenz – wie etwa auch die Checkliste zu Windows 10 – sind zu berücksichtigen. Unter Einhaltung dieser Verfahrensvorkehrungen wären datenschutzrechtliche Sanktionen gegen die Nutzer solcher Cloud-Dienste wohl widersprüchlich und unzulässig („venire contra factum proprium").

Soweit es freilich über diese speziellen IT-Produkte von Microsoft hinausgeht, etwa bei der Wahl eines allgemeinen Cloud-Anbieters für kommunale Verwaltungsdienstleistungen, dürften Angebote deutscher/europäischer Unternehmen regelmäßig vorrangig sein.[97] Schon aufgrund ihrer spezifischen Gesetzesbindung bieten sich auch öffentlich-rechtlich organisierte IT-Dienstleister oder kommunale Rechenzentren an.

[97] Es hat sicher auch mehr als symbolische Bedeutung, dass die Bundesregierung für die Implementierung der Corona-Warn-App auf eine Zusammenarbeit mit der Deutschen Telekom (neben SAP) setzte.

ANHANG: Exkurs zum Cloud Treuhandmodell Microsoft Cloud Deutschland

Den datenschutzrechtlichen Bedenken bzgl. der Beauftragung eines amerikanischen Cloud-Anbieters, selbst bei Verwendung ausschließlich in Europa/Deutschland befindlicher Server, wurde bisher durch das Angebot der sog. Microsoft Cloud Deutschland, einer Art Treuhändermodell, begegnet. Zwar wird ein solches Modell in Deutschland derzeit von keinem Anbieter zur Verfügung gestellt. Aufgrund des besonders hohen Sicherheitsniveaus dieses Modells, wenngleich auch dieses aus Praktikabilitätsgründen kritisiert wurde, soll die Nutzbarkeit eines solchen Modells im Rahmen der Vorschriften der mittlerweile geltenden DSGVO kurz dargestellt werden.

Im Vordergrund des Modells stand der möglichst weitgehende Entzug der Zugriffsmöglichkeiten durch amerikanische Anbieter und somit auch amerikanischen Ermittlungsbehörden.

Technische Seite

Nach Aussagen der beteiligten Unternehmen (Microsoft und T-Systems International GmbH) hatten die Kundendaten nicht die in Deutschland stehenden Rechenzentren verlassen.[98] Die Datenverarbeitung fand daher beschränkt auf diese beiden Standorte statt. Die Datenherrschaft der von Microsoft verwalteten Cloud wurde einem Datentreuhänder (T-Systems) übertragen.[99] T-Systems hatte ihren Sitz in Deutschland und unterfiel somit nicht der persönlichen Gerichtsbarkeit der USA.[100] Durch den Einsatz einer Verschlüsselung der Clouddaten und dem ausschließlichen Schlüsselbesitz des Treuhänders[101] wurde so Microsoft bereits der faktische Zugriff auf die Daten verwehrt.[102] Das bedeutete, dass Microsoft im Regelbetrieb keinen Zugriff auf die Kundendaten hatte. Die Beschäftigten von Microsoft waren insofern auch nicht im Besitz von administrativen Top-Level-Rechten, die einen Zugriff auf die Daten ohne Mitwirkung seitens T-Systems erlaubt hätten. Einen Zugriff hatte das Unternehmen insofern nur dann, wenn der sogenannte „Datentreuhänder“ T-Systems den Zugriff auf die gespeicherten Daten freischaltete.

---

[98] *Microsoft TechNet,* https://blogs.technet.microsoft.com/ralfwi/2015/12/08/microsoft-cloud-deutsche-datentreuhand/. So auch *Schwartz/Peifer,* CR 2017, 165, 169 f.
[99] *Schwartz/Peifer,* CR 2017, 165, 169 f.
[100] *Schwartz/Peifer,* CR 2017, 165, 170.
[101] *Rüdinger,* ZDNet, http://www.zdnet.de/88287109/deutschland-cloud-datentreuhaendervertrag-soll-unternehmen-weg-in-die-cloud-ebnen/.
[102] *Schwartz/Peifer,* CR 2017, 165, 171.

Wenn im Ausnahmefall Microsoft auf Antrag Zugriff auf die Kundendaten gewährt wurde, beendete T-Systems unverzüglich den Datenzugriff, sobald das technische Problem gelöst wurde.[103] Eine solche Ausnahme wurde etwa insbesondere für die Wartung (Softwareupdates) gemacht.[104] Ansonsten kam eine Ausnahme zum Zugriff seitens Microsoft nur in Betracht, wenn der Kunde oder deutsche Rechtsvorschriften dies erlaubten.[105]

Rechtliche Beurteilung

Das Verhältnis des Cloud-Anbieters zum Kunden wird bei dem Treuhändermodell als Auftragsverarbeitung im Sinne des Art. 28 DSGVO einzuordnen sein. Daher bedarf auch dieses Modell für die Verarbeitung für die Rechtmäßigkeit der Datenverarbeitung keine besondere Rechtfertigung durch den Kunden. Zumindest wird amerikanischen Unternehmen durch den weitgehenden Entzug faktischer Zugriffsmöglichkeiten die Herausgabe geschützter Daten an amerikanische Behörden erschwert, ganz ausgeschlossen werden kann sie aufgrund technischer Erfordernisse (etwa Instandhaltung etc.) allerdings nicht. Bei realistischer Ausgestaltung des Treuhändermodells wird nämlich zumindest eine Ausnahmeregelung des Zugriffsverbots für Wartung und Fehlerbehebung unumgänglich sein. Zumindest unter gewissen Umständen bleibt amerikanischen Cloud-Anbietern dann die tatsächliche Zugriffsmöglichkeit.

Grundsätzlich wäre das Treuhandmodell eine rechtlich weitgehend sichere Variante. Zurückführend auf die Erkenntnisse aus der Microsoft Office Pro Plus-Studie wird ein solches Modell gerade in Bezug auf die Erhebung von Diagnosedaten aber nur schwer umsetzbar sein. Diagnosedaten, zu denen der Zugang durch den Cloud-Anbieter von vornherein faktisch verhindert wird, hat für den Anbieter nur noch wenig wert. Gerade aus Gründen der Systemgewährleistung und ständigen Wartung werden diese Daten allerdings erhoben.

Mit Beginn des Jahres 2019 hat Microsoft den Betrieb der Microsoft Cloud Deutschland weitgehend eingestellt und das Angebot für Neukunden vom Markt genommen. Altkun-

[103] *Oltmanns-Mack,* ORBIT, http://blog.orbit.de/2016/11/10/microsoft-cloud-deutschland-powered-t-systems/.
[104] *Schwartz/Peifer,* CR 2017, 165, 170.
[105] *Schwartz/Peifer,* CR 2017, 165, 170.

den ist bisher die Aufrechterhaltung der Cloud inklusive erforderlicher Sicherheitsupdates versprochen worden.[106] Mitunter war die Cloud deswegen als problematisch betrachtet worden, weil sie nur schlecht mit anderweitigen internationalen Cloud-Angeboten integrierbar war.[107] Microsoft selbst begründete die Einstellung der Cloud mit der in Deutschland nur geringen Nachfrage.[108] Derzeit ist das erneute Angebot von Cloud-Diensten nach dem Treuhändermodell nicht beabsichtigt.

[106] *Microsoft,* https://www.microsoft.com/de-de/cloud/deutsche-cloud.
[107] *Schüler,* heise, https://www.heise.de/newsticker/meldung/Auslaufmodell-Microsoft-Cloud-Deutschland-4152650.html.
[108] *Kling,* ZDNet, https://www.zdnet.de/88341229/microsoft-cloud-deutschland-steht-fuer-neukunden-nicht-mehr-zur-verfuegung/.