DataAgenda-Arbeitspapier 27, 03/2021

DataAgenda - das Informationsportal zum Datenschutzrecht

Präsentiert von DATAKONTEXT

www.DataAgenda.de

@dataagenda

Nutzung US-amerikanischer Bürosoftware seit Schrems-II

I. Das EuGH-Urteil v. 16. Juli 2020 „Schrems II“

Seit *Schrems-II* kann das EU-US-Privacy-Shield-Abkommen, wegen der aus der Sicht des *EuGH* überzogenen Massenüberwachung durch US-amerikanische Sicherheitsbehörden wie der *NSA*, Datenübermittlungen in die USA nicht mehr rechtfertigen. Aus demselben Grund scheiden dem *EuGH* zufolge auch Standardvertragsklauseln (Art. 46 DS-GVO) ohne weiteres als Legitimation für eine Datenübermittlung in die USA aus.

II. Auswirkungen auf die Rechtmäßigkeit US-amerikanischer Software

Für US-amerikanischer Softwareanbieter gibt es seither nur noch zwei Möglichkeiten, Verstöße gegen die DS-GVO zu verhindern. Eine Verlagerung der Datenverarbeitung in die EU oder die Implementiert zusätzlicher Sicherheitsmaßnahmen, um einen übermäßigen Zugriff amerikanischer Behörden auszuschließen. Ersteres hat bspw. der *Microsoft-Konzern* schon vor einigen Jahren in die Wege geleitet, Daten von Europäern werden seither, etwa bei der Nutzung von Diensten wie *Microsoft 365*, ausschließlich in der EU verarbeitet. Zumindest die **offline Nutzung** von ***Microsoft 365*** ist damit nach wie vor **rechtmäßig**.

Den in multilateralen Konzernen unausweichliche Datenaustausch mit den USA kann diese Lösung jedoch naturgemäß nicht legitimeren. Ebenso wenig bietet eine europäische Datenverarbeitung Schutz vor dem sog. Cloud-Act, der Anbieter von Kommunikations- und Cloud-Angeboten dazu verpflichtet, Anfragen amerikanischer Behörden Folge zu leisten, unabhängig davon, wo die Daten gehostet werden. In diesen Fällen bedarf es demnach zusätzlicher Schutzmaßnahmen auf Seiten der Anbieter. Der *EDSA* geht gegenwärtig davon aus, dass hierfür nur eine technische Sicherung genügt, d.h. insb. eine clientseitige Verschlüsselung. Eine solche ist indes nicht in jedem Fall, zumindest nicht ad hoc, realisierbar. Die Nutzung von amerikanischen Cloud-Angeboten wie bspw. ***OneDrive*** ist damit gegenwärtig **rechtswidrig**.

III. Konsequenzen für den Einsatz der Software

Der Einsatz entsprechender Anwendungen kann dennoch in vielen Fällen nicht einfach verboten werden. Immerhin sind US-amerikanische Produkte in der Regel **Marktstandard**. Zudem fehlt es an **wettbewerbsfähigen Alternativen**. Ein **Verzicht** auf die Software ist daher häufig **kein realistischen Szenario**. Dennoch drohen Aufsichtsbehörden immer wieder unspezifisch Nutzungsuntersagungen und Sanktionen an. Unternehmen haben nun verschiedene Möglichkeiten sich zu verhalten.

DATAKONTEXT GmbH • Augustinusstraße 9d • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

1. Einholung von Einwilligungen

Eine Möglichkeiten die Datenübermittlung in die USA zu legitimieren wäre diese auf Art. 49 Abs. 1 lit. a DS-GVO zu stützen. Das hieße Einwilligungen der betroffenen Personen in die Drittlandübermittlung einzuholen. Diese müssten aber nicht nur in Kenntnis der Risiken und eines nicht vorhandenen, angemessenen Datenschutzniveaus erfolgen, sondern auch freiwillig. Dass **Mitarbeiter** die entsprechende Einwilligung freiwillig erteilen können, erscheint indes **fraglich**. Immerhin könnte der jeweilige Arbeitnehmer bei einer Weigerung die digitale Infrastruktur des Unternehmens nicht länger nutzen und damit in vielen Fällen kaum noch produktiv arbeiten.

Eine Einwilligung der **Kunden** einzuholen wäre hingegen **denkbar** und könnte zumindest vor Schadensersatzansprüchen von außen schützen. Auch das ist allerdings bisher nicht gesichert.

2. Berufung auf die fehlende Zumutbarkeit eines Verzichts

Alternativ könnte sich auf die fehlende Zumutbarkeit des Verzichts auf die entsprechende Software berufen werden. Sowohl eine **Nutzungsuntersagung** als auch eine Sanktionierung wg. eines Verstoßes gegen die DS-GVO sind **rechtswidrig**, **wenn** den Verantwortlichen ein **normgerechtes Verhalten unzumutbar** ist. Mit Blick auf die **Rechenschaftspflicht** aus Art. 5 Abs. 2 DS-GVO haben die Verantwortlichen indes **intern darzulegen** und zu begründen, warum ein Anbieterwechsel gegenwärtig nicht im Bereich des Möglichen liegt. Diese **Prüfung ist** regelmäßig **zu wiederholen**. Sollte die Aufsicht Schritte gegen das Unternehmen einleiten, sind die Erwägungen der Aufsicht zur Verfügung zu stellen (Art. 58 Abs. 1 lit. a DS-GVO)

3. Berufung auf eine interne Risikoabwägung

Das Halten der Daten innerhalb der EU darf zudem nicht zu einem Abfall der Sicherheitsstandards führen. Ein **Verbot** amerikanischer Software wäre daher auch dann **ermessensfehlerhaft**, **wenn** die zur Verfügung stehenden europäischen Anbieter, bspw. mit Blick auf unausgereifte Verschlüsselungstechniken, das **Risiko** für Betroffene **erhöhten**. Zudem ist zu berücksichtigen, dass es **bisher kaum** zu **Anfragen** nach dem Cloud-Act gekommen ist. Auch im Interesse der Datensicherheit kann daher u.U. von einem Anbieterwechsel abgesehen werden. Die entsprechende **Risikoabwägung** ist indes ebenso wie die fehlende Zumutbarkeit nach Art. 5 Abs. 2 DS-GVO darzulegen und regelmäßig zu wiederholen.

4. Ergänzung der Datenschutzfolgeabschätzung sowie der Datenschutzerklärung

In jedem Fall sollten ergänzend **Datenschutzfolgenabschätzung** und **Datenschutzerklärung** angepasst werden. Die Datenübermittlung in die USA sollte in das Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden. Zudem muss darauf hingewiesen werden, dass unklar ist, ob amerikanische Behörden Zugriff auf die Daten nehmen bzw. ein angemessenes Datenschutzniveau hier nicht garantiert werden kann.

IV. Rechtsschutzmöglichkeiten

Da ein latentes Sanktionsrisiko trotz allem besteht, kann ergänzend eine **vorbeugende Feststellungsklage** vor dem Verwaltungsgericht erhoben werden. Hierdurch könnte gerichtlich festgestellt werden, dass ein Nutzungsverbot US-amerikanischer Software ermessenfehlerhaft wäre und gleichsam eine Sanktionierung verhindert werden.

DATAKONTEXT GmbH • Augustinusstraße 9d • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

Seminartipps zum Arbeitspapier

GDD-Forum: Microsoft und die Datenschutzdiskussion

Microsoft Office, Windows 10 und Cloud Dienste

- Office 365 und die Versionen
- Naming and Shaming
- Windows 10 und Telemetrie
- DSFA Niederlande
- Cloud Dienste (Teams, SharePoint, Exchange, Azure)

Was tut Microsoft für den Datenschutz?

- Standard-Vertragsklauseln und geeignete Garantien
- Darstellung welche Daten wie und wo verarbeitet werden
- Welche Schutzmaßnamen gibt (z.B. Verschlüsselte Speicherung im One Drive)
- Was ist MyAnalytics und Workplace Analytics?
- Double Key Encryption und Application Guard für Office

Rechtliche Beurteilung von Microsoft 365 aus Sicht der Aufsichtsbehörde

- Schrems II und die Auswirkungen auf ASV in Europa mit amerikanischen Dienstleistern
- Ist es ein Unterschied, ob ein US-Dienstleister die Daten in USA oder in Europa verarbeitet?
- Sind die geeigneten Garantien von MS ausreichend?

Weitere Infos finden Sie hier.

Microsoft 365/Office 365 datenschutzrechtlich bändigen

Microsoft 365 (der neue Name von Office 365) gilt datenschutzrechtlich als kritisch. Dies liegt insbesondere an den Telemetrie-Funktionen. Microsoft 365 kommuniziert im Hintergrund mit der Microsoft Infrastruktur. Mit geeigneten Konfigurationseinstellungen kann dies unterbunden werden.

Die einzelnen Module von Microsoft 365 werden in diesem Online-Kompaktkurs erläutert. Die unterschiedlichen Möglichkeiten zu Nutzung der Module werden unter datenschutzrechtlichen Gesichtspunkten diskutiert.

Weitere Infos finden Sie hier.

DataAgenda
ist das Informationsportal zum Datenschutzrecht und fokussiert sich auf die inhaltlichen Entwicklungen in diesem Feld. Das DataAgenda-Experten-Team bietet Videos, News, Whitepaper und Seminartipps rund um den Datenschutz.

Datakontext
ist einer der führenden Fachinformationsdienstleister in den Bereichen Datenschutz und IT-Sicherheit und bietet Kompetenz aus einer Hand: Fachbücher, Fachzeitschriften und Seminare, Zertifizierung und Beratung.

Autoren

Prof. Dr. Rolf Schwartmann
Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V (GDD), Leiter der Kölner Forschungsstelle für Medienrecht (TH Köln) und Mitglied der Datenethikkommission.

Dr. Tobias Jacquemain, LL.M.
Mitglied der Geschäftsführung der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

DATAKONTEXT GmbH • Augustinusstraße 9d • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com