3562/J XXVII. GP

Eingelangt am 25.09.2020

Anfrage

der Abgeordneten Mag[a]. Dr[in]. Petra Oberrauner, Genossinnen und Genossen

an den Bundesminister für Finanzen

betreffend: **Umsetzungsstand EuGH C-311/18**

Mit dem EuGH-Urteil C-311/18 wurde der Datenverkehr zwischen der Europäischen Union und Drittstaaten, soweit im Drittland nicht dasselbe Schutzniveau für Europäische Bürger besteht, als im Widerspruch zur DSGVO erkannt[1]. Bereits im Jahr 2015 hatte der EuGH (C-362/14) die Entscheidung der Europäischen Kommission, dass das Safe-Harbor Abkommen zwischen der EU und den USA ein angemessenes Schutzniveau gewährleisten würde, für ungültig erklärt. Sogenannte Standardvertragsklauseln sind gültig, so lange sie wirksame Mechanismen enthalten, die ein der DSGVO ähnliches Schutzniveau bewirken. Das Problem entsteht aber durch Überwachungsprogramme von Drittstaaten, die in die Datenschutzrechte europäischer Bürger eingreifen, vor allem dadurch, dass die nationalen Rechtsvorschriften des Drittstaates den EU-Bürgern keine gerichtlich durchsetzbare Rechte einräumen.

Der Datenschutzaktivist Maximilian Schrems erkannte das Problem in der Übermittlung seiner Facebook-Daten von Facebook Irland an amerikanische Server, denn amerikanische Unternehmen sind dazu verpflichtet, die ihnen übermittelten personenbezogenen Daten den Sicherheitsbehörden/Geheimdiensten zu übermitteln. Dieses widerspricht aber dem Grundrechtsschutz der Art. 7 und Art. 8 der Europäischen Grundrechte-Charta, die Achtung des Privat- und Familienlebens sowie den Schutz personenbezogener Daten regeln. Diese Rechte sind durch Art. 47 geschützt und vor einem unparteiischen europäischen Gericht durchsetzbar. Die Klage von Herrn Schrems in Irland führte zu Vorlagefragen an den EuGH, wobei der vorlegende High Court auf ein zuvor im Jahr 2017 gefälltes Urteil verwies, in welchem die nachrichtendienstliche Tätigkeit der USA bereits geprüft worden war[2]. Auch das US-amerikanische Recht unterscheidet zwischen US-Bürgern, die durch die Verfassung der Vereinigten Staaten gegen anlasslose Überwachung geschützt sind (4. Zusatzartikel), und Nicht-US-Bürgern.

Die Auslandsüberwachung der Vereinigten Staaten wird, umgangssprachlich formuliert, in Bausch- und Bogen durchgeführt, wobei Nutzerdaten nicht nur von den Internetfirmen an die US-Behörden übermittelt werden müssen, sondern es werden auch die

1 http://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18
2 s. Absätze 51ff, Schlussanträge des Generalanwaltes

Telekommunikationsdaten an den Infrastrukturknotenpunkten (Unterseekabel, Switches, Router) kopiert um sie dann filtern zu können. Dabei werden die Daten von US-Bürgern durch den Schutz der amerikanischen Verfassung anders behandelt als jene der anderen Staaten. Bei ersteren muss es im Einzelfall einen konkret bewilligten Überwachungsanlass geben, bei allen anderen reicht ein jährlich bewilligtes Überwachungsvorhaben.

Der EuGH stellt nun vereinfacht formuliert fest, dass

a die gewerbliche Datenübermittlung personenbezogener Daten von einem EU-Unternehmen an einen Drittstaat dem europäischen Datenschutzrecht (DSGVO) unterliegt (Pkt 1, RN 89),

b die DSGVO auch bezüglich der Garantien und wirksamen Rechtsbehelfe in einem Nicht-EU-Land gilt (Pkt 2, RN 105),

c die Datenschutzbehörde verpflichtet ist die Datenübermittlung an Drittstaaten zu verbieten oder auszusetzen, wenn das Schutzniveau der DSGVO und der Grundrechtecharta nicht gewährleistet ist (Pk 3, RN 121), und

d der Datenschutzschildbeschluss (Privacy-Shield EU-USA) ungültig ist (Pkt 5, Rn 199ff).

Zusammengefasst: Da die US-Behörden über die Internetdatenstaubsauger ihrer Geheimdienste Zugang zu allen Metadaten und allen Kommunikationsdaten der EU-Bürger, die über amerikanische Infrastruktur gesendet werden, haben und sich die EU-Bürger nach amerikanischem Recht nicht dagegen aussprechen können, sind die gängigsten bzw. automatischen Datenübermittlungen in die USA rechtswidrig (es sei denn der Benutzer schickt wissentlich Mails dorthin, Einreisedaten oder z.B. Bankdaten für Überweisungen).

Das EuGH-Urteil C-311/18 datiert mit 16.07.2020. Im Zuge der Covid-19-Krise wurden vielfach alternative Kommunikationsinstrumente eingesetzt, die sich wahrscheinlich weitgehend bewährt haben und nun Teil des Alltags werden. Das betrifft nicht nur Whatsapp-Gruppen für die chat-artige Kommunikation, sondern auch die eingesetzten Server- und Cloud-Technologien, die dem zentralen Datenaustausch mit den Österreicherinnen und Österreichern dienen. Letztlich ist es dabei egal welche Anbieter gewählt werden, die gängigsten Lösungen sind beispielsweise Google-Mail, -Cloud und -Docs-Anwendungen, Microsofts-Office-365-Cloud (Azure)-Produkte (Word, Excel, Outlook), Apple iCloud, Messengerdienste von Whatsapp, Facebook, Telekonferenz-VOIP-Tools wie Zoom, Microsoft-Teams, Skype, Face-Time, Amazon-Alexa-Telefonie, Cisco-Web-Ex-Meeting usw.

Setzen Ministerien und nachgelagerte Behörden auf diese Softwareprogramme, werden Daten österreichischer Bürgerinnen und Bürger verarbeitet und gespeichert. Diese Verarbeitung muss aber den europäischen Datenschutzstandards entsprechen, daher letztlich in der EU vorgenommen werden. Andernfalls landen diese Daten auf Serverinfrastrukturen außerhalb der EU, und die betroffenen Personen haben de facto keine Möglichkeit gerichtlich durchzusetzen, dass ihre Daten geschützt sind.

Dabei geht es nicht allein um die Daten, die in die USA übermittelt werden, sondern um jeden Drittstaat, der aus Sicht der EU nicht das gleiche Schutzniveau für persönliche Daten hat.

Die unterzeichnenden Abgeordneten stellen daher nachstehende

Anfrage:

1 Welche Schlussfolgerungen haben Sie aus dem Judikat EuGH C-311/18 für die unmittelbare Tätigkeit ihres Ministeriums bzw. nachgelagerter Dienststellen gezogen?

2 Arbeiten Sie in ihrem Ministerium oder in den - ihrem Ministerium nachgelagerten - Dienststellen mit Software die möglicherweise Daten von Österreicherinnen und Österreichern rechtswidrig an ausländische Server außerhalb der EU schickt?
Wenn ja, um welche Software handelt es sich und welche Maßnahmen haben Sie getroffen- bzw. planen Sie, um die betroffenen Menschen besser zu schützen?

3 Haben Sie Handlungsempfehlungen ausgearbeitet, damit ihr Ministerium und ihm nachgelagerte Dienststellen technisch in die Lage versetzt werden die persönlichen Daten von österreichischen Bürgerinnen und Bürgern zu schützen und auf Servern innerhalb der EU zu speichern? Wenn nein, warum nicht?

4 Haben Sie Handlungsempfehlungen ausgearbeitet, wie ihr Ministerium und ihm nachgelagerte Dienststellen vorgehen müssen, wenn sie bislang Software eingesetzt haben, bei der technisch nicht ausschließbar ist, dass persönliche und sensible Daten von österreichischen Bürgerinnen und Bürgern auf Servern außerhalb der EU in Drittstaaten gespeichert oder verarbeitet werden? Wenn nein, warum nicht?

5 Haben Sie Handlungsempfehlungen ausgearbeitet, wie ihr Ministerium und ihm nachgelagerte Dienststellen vorgehen können, um Softwareumstellungen vorzunehmen, mit denen die Daten der österreichischen Bürgerinnen und Bürger auf Servern innerhalb der EU gespeichert oder verarbeitet werden, damit sie sich EU-Datenschutzrechts konform verhalten? Wenn nein, warum nicht?

6 Haben Sie mit Ihren IT-Beratern im Ministerium das Problem der nicht rechtskonformen Verarbeitung von Daten durch die von ihrem Ministerium und ihm nachgelagerte Dienststellen eingesetzte Software erhoben, geprüft, analysiert und daraus Schlussfolgerungen hinsichtlich der rechtlichen Konsequenz und der verwendeten Software gezogen? Wenn ja, zu welchem Ergebnis sind sie gekommen? Wenn nein, warum nicht?

7 Haben Sie mit Ihren Regierungskollegen, insbesondere der Bundesministerin für Digitalisierung und Wirtschaftsstandort oder der Bundesministerin für EU und Verfassung im Bundeskanzleramt eine Lösung für dieses Problem erarbeitet? Wenn nein, warum nicht?

8 Gibt es eine Empfehlung ihres Ministeriums zur Einsparung von IT-Kosten auf Cloudprodukte privater Anbieter bzw. bestimmter Unternehmen zu setzen? Wurde diese Empfehlung an die neue Rechtslage angepasst? Wenn nein, warum nicht? Wenn ja, mit welchem Inhalt (bitte um Beilage des aktuellen Textstandes zu Anfragebeantwortung)? Gibt es angesichts der aktuell geänderten Rechtslage Überlegungen im Ministerium den Einsparungskurs bei der IT-Soft- und Hardware zu überdenken?