www.jusletter-it.eu

Simon Schlauri

Die sogenannte «Treuhandlösung» und das Schrems-II-Urteil

Beitragsart: TechLawNews by Ronzani Schlauri Attorneys
Region: Schweiz
Rechtsgebiete: Datenschutz

Zitiervorschlag: Simon Schlauri, Die sogenannte «Treuhandlösung» und das Schrems-II-Urteil, in: Jusletter IT 16. Dezember 2021

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

1. Die Schrems-Rechtsprechung des EuGH

[1] Vor rund fünf Jahren vertrat der Autor in einem TechLawNews-Beitrag die Auffassung, nach dem damaligen Ende der Safe-Harbor-Regelung durch das Schrems-I-Urteil[1] sei ein Ersatz der Safe-Harbor-Regeln durch die sogenannten «Standardklauseln» nicht wirksam. Dies weil angesichts der damaligen Rechtslage in den USA sich ein US-Unternehmen gar nicht gültig verpflichten könne, den europäischen Datenschutz einzuhalten; es liege eine Simulation oder zumindest Unmöglichkeit vor.[2]

[2] Die Datenübermittlung in unsichere Drittländer ist nach schweizerischem und europäischem Datenschutzrecht u.a. dann zulässig, wenn der für die Bearbeitung verantwortliche Empfänger ausreichende Garantien (vertraglicher Natur) hinsichtlich des Schutzes der Privatsphäre abgibt. Die EU-Kommission und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte EDÖB haben in der Folge Standardverträge (die genannten «Standardklauseln») veröffentlicht, die zu diesem Zweck genutzt werden können. Deren Verwendung ist heute im Datenverkehr mit unsicheren Drittländern etabliert.

[3] Die im damaligen TechLawNews-Beitrag vertretene Position des Autors wurde in der Folge durch das Schrems-II-Urteil[3] bestätigt: Zunächst befand das Gericht, die USA könnten weiterhin nicht als sicheres Drittland gelten. Zu beachten ist sodann, dass eine Übertragung an eine US-Anbieterin, selbst wenn vertraglich versprochen wird, dass die Daten nur in der Schweiz oder der EU gespeichert werden, oft einer Übertragung in die USA gleichzustellen ist. Dies deshalb, weil US-Anbieterinnen aufgrund der US-amerikanischen Gesetzeslage verpflichtet sein können, Daten, selbst wenn sie in der Schweiz oder der (als sicher geltenden) EU gespeichert werden, an US-Behörden (zu denken ist an Strafermittler oder Geheimdienste) herauszugeben.[4]

[4] Zu beachten ist eine weitere Aussage des Gerichts: Es befand, die Standardklauseln allein seien nicht grundsätzlich geeignet, das Problem zu beheben, dass die USA als unsicheres Drittland gelten. Bei der Beurteilung, ob durch die Verwendung der Standardklauseln ein angemessenes Schutzniveau geschaffen werde, sei insbesondere ein etwaiger Zugriff der Behörden des Drittlands auf die übermittelten personenbezogenen Daten zu berücksichtigen.[5] Da diese Standardklauseln ihrer Natur nach keine Garantien bieten können, die über die vertragliche Verpflichtung, für die Einhaltung des unionsrechtlich verlangten Schutzniveaus zu sorgen, hinausgehen, könne es je nach der in einem bestimmten Drittland gegebenen Lage erforderlich sein, dass der

1 EuGH, Urteil vom 16. Oktober 2015, Rs. C-362/14, Schrems vs. Data Protection Commissioner.

2 S. Schlauri,Internationaler Datenaustausch: Entwicklungen nach dem Ende von Safe Harbor, in: Jusletter IT 25. Februar 2016.

3 EuGH, Urteil vom 16. Juli 2020, Rs. C-311/18, Facebook Irland und Schrems.

4 «U.S. CLOUD Act»; dazu etwa M. Schwarz, der US CLOUD ACT, EF 4/20, 193 ff.

5 EuGH (FN 3), Rz. 105.

Verantwortliche zusätzliche Massnahmen ergreift, um die Einhaltung dieses Schutzniveaus zu gewährleisten.[6]

2. Der risikobasierte Ansatz der neuen Standarddatenschutzklauseln

[5] Unter anderem als Konsequenz aus dem Schrems-II-Urteil wurden die Standardklauseln überarbeitet. Sie folgen nun einem risikobasierten Ansatz und verlangen im Fall möglicher Eingriffe von ausländischer Behörden eine dokumentierte Prüfung und Entscheidung darüber zu treffen, inwieweit weitere Massnahmen zum Schutz der Daten erforderlich sind (mehr dazu bei Daniel Ronzani, The New Standard Contractual Clauses in Practice, in dieser Nummer von Jusletter IT). Gemäss Ziff. 14 ist ein sogenanntes Transfer Impact Assessment (TIA) durchzuführen.[7]

[6] Auch der EDÖB verlangt in seiner «Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug (nach Art. 6 Abs. 2 lit. a DSG)» vom Juni 2021 organisatorische und technische Massnahmen, die die Behördenzugriffe auf die übermittelten Personendaten im Zielland *faktisch verhindern*.[8]

[7] Die Zürcher Datenschutzbeauftragte verfolgt einen vergleichbaren Ansatz: Im Fall der Bearbeitung von besonders schützenswerten Personendaten in Ländern ohne angemessenes Datenschutzniveau muss beispielsweise das Schlüsselmanagement beim Auftraggeber verbleiben.[9] Dies bedeutet, dass Applikationen, die in der Cloud mit den Daten arbeiten und damit Zugriff auf unverschlüsselte Daten benötigen (was eigentlich fast immer der Fall ist), bei der Bearbeitung besonders schützenswerter Personendaten nicht mehr genutzt werden können.

[8] Kurz: Die Cloud-Anbieterin darf keinen Zugriff auf die Daten erhalten, was mit geeigneten organisatorischen und technischen Massnahmen zu realisieren ist. Der einzige Weg, dies realistischerweise zu gewährleisten, liegt in der Verschlüsselung der Daten, und zwar vor dem Upload in die Cloud. Die Kontrolle über die Entschlüsselungsschlüssel muss dabei vollständig in der Hand des Kunden bleiben.

3. Datentransfers in die USA bleiben problematisch

[9] Damit werden aber zugleich auch die meisten Cloud-Anwendungen ausgeschlossen, denn gerade jene Anwendungen, in denen die Daten in der Cloud auch bearbeitet werden sollen, sind so nicht mehr möglich.

[10] Genau zu diesen Anwendungen gehören nun aber die funktionsmächtigen Cloud-Angebote der US-Hyperscaler wie auch Lösungen wie das cloudbasierte Office365. Just bei ihnen lässt sich das anfangs geschilderte Problem der ausländischen Behördenzugriffe auf den ersten Blick also gar nicht lösen.

---

6 A.a.O., Rz. 133.

7 Vertiefend dazu in der vorliegenden Nummer von Jusletter IT Daniel Ronzani, The New Standard Contractual Clauses (SCC) in Practice.

8 tinyurl.com/4prs58ax.

9 Datenschutzbeauftragte des Kantons Zürich, Verschlüsselung der Daten im Rahmen der Auslagerung – unter Inanspruchnahme von Informatikleistungen und unter Berücksichtigung der Geheimnispflichten, tinyurl.com/ybaft3tf.

4. Revival der «Treuhandlösung»?

[11] Es sei denn, man setzt konsequenterweise auf einen Cloud-Anbieter, der gar nicht der US-Jurisdiktion untersteht. Hier kommt die sogenannte «Treuhandlösung» ins Spiel, welche insbesondere Microsoft seit 2016 in Kooperation mit der Deutschen Telekom AG anbietet.

[12] Bei der Treuhandlösung wird die Cloud-Software von Microsoft nicht mehr durch Microsoft selber gehostet, sondern («treuhänderisch») durch ein drittes Unternehmen mit Sitz in der EU. Microsoft erhält nur Zugriff auf die gespeicherten Daten, um Support zu leisten, und auch dies erfolgt immer gemäss Vieraugenprinzip. Sowohl der EU-Anbieter (als Nicht-US-Unterhemen), als auch Microsoft selber (weil sie nicht mehr als Hoster auftritt), sind damit dem Zugriff der US-Behörden entzogen.

[13] Problematisch an der Treuhandlösung ist, dass Microsoft offenbar wenig Anreiz hat, diese auf einem mit ihren normalen Angeboten vergleichbaren technischen Niveau zu halten, und dass sie erheblich teurer ist. Die Nachfrage blieb damit beschränkt. 2018 hiess es denn auch zwischenzeitlich, die Treuhandlösung sei ein Auslaufmodell, und es würden keine neuen Kunden mehr aufgenommen.[10]

[14] Die Frage bleibt sodann, ob Daten in einer «Treuhand-Cloud» tatsächlich auch beim jeweiligen Hoster bleiben. Eine Untersuchung der Computerzeitschrift iX im Jahr 2018 förderte jedenfalls zutage, dass selbst unter der Treuhandlösung der Deutschen Telekom weiterhin auch Datenaustausch mit MS-Servern erfolgte, was den zertifizierenden Unternehmen wohl durch fahrlässige Unaufmerksamkeit entgangen war.[11] Solches wäre natürlich zu verhindern.

[15] Erst neulich war zu lesen, dass es unter dem Eindruck des Schrems-II-Urteils zu einem Ausbau der Treuhandlösung kommt. In Frankreich bieten mittlerweile Orange und Capgemini eine vergleichbare Hostinglösung für MS-Clouddienste an, und auch die deutsche Bundesregierung erhielt einen entsprechenden Vorschlag von MS.[12]

[16] Damit sollte sich Schweizer Unternehmen und Behörden im Grundsatz die Möglichkeit bieten, auf die entsprechenden Angebote in Deutschland und Frankreich abzustellen, die bekanntlich ein ausreichendes Datenschutzniveau gewährleisten. Alternativ könnten sich Schweizer Datenschutzbeauftragte zusammentun und bei den relevanten US-Anbieterinnen vorstellig werden, um auch für die Schweiz eine Treuhandlösung zu fordern. Sie böte jedenfalls die Möglichkeit, bei der datenschutzkonformen Nutzung US-amerikanischer Clouddienste endlich Nägel mit Köpfen zu machen.

---

10 Vgl. etwa H.-P. Schüler, Auslaufmodell: Microsoft Cloud Deutschland, Heise Newsticker vom 31. 8. 2018, tinyurl.com/29ccvpt4.

11 L. Grunwald, Glauben statt wissen, iX 9/2018, 82, tinyurl.com/2p8rup89.

12 C. Wölbert, Auf dem Weg in die Wolke, c't 14/2021, 136, tinyurl.com/y8z2mhm7.