Anwendungshinweise der DSK zum Angemessenheitsbeschluss des EU-U.S. Data Privacy Framework - Der TLfDI weicht vom Votum der DSK ab und nimmt Stellung!

Dienstag, 05 September 2023

https://www.datenschutz.de/anwendungshinweise-der-dsk-zum-angemessenheitsbeschluss-des-eu-u-s-data-privacy-framework-der-tlfdi-weicht-vom-votum-der-dsk-ab-und-nimmt-stellung/

Pressemitteilung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) vom 04.09.2023

Bereits am 14. Juli 2023 hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in seiner Pressemittelung zu EU-U.S. Data Privacy Framework (DPF) vor zu großer Euphorie gewarnt.

Die Datenschutzkonferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) verabschiedete jetzt ein Papier mit Anwendungshinweisen zum Angemessenheitsbeschluss des Data Privacy Frameworks.

Dieses Framework erlaubt den Datentransfer personenbezogener Daten in die USA, ohne dabei zusätzliche Maßnahmen treffen zu müssen. Empfänger sind zertifizierte US-Organisationen (meist Unternehmen). Der TLfDI verweist zur inhaltlichen Information, welche Regelungen und Beschwerdemöglichkeiten für Verantwortliche und Betroffene existieren auf das oben genannte DSK-Papier. Hierin finden sich insbesondere in Kapitel III Eingriffsmöglichkeiten bei Beschwerden

- gegenüber zertifizierten Unternehmen,
- bei Verdacht auf rechtswidrige Datenverarbeitung im Fall von Strafverfolgung,
- bei Verdacht auf rechtswidrige Datenverarbeitung im Fall der „Sicherstellung der nationalen Sicherheit“.

Sind damit Datentransfers in die USA von nun an problemlos möglich? Kann nun alles mit einer Vertragsunterschrift bedenkenlos bewilligt werden? Nein. Es gibt weitere Punkte zu bedenken und dies ist auch der Grund, weshalb der TLfDI den Anwendungshinweisen der DSK leider nicht zustimmen konnte, da diese die Punkte allenfalls sehr dezent aufgreifen .

Daher möchte der TLfDI zu den Anwendungshinweisen zwei Punkte ergänzen.

1. Pflichten des Verantwortlichen:
Bei Nutzung von US-Anbietern (wie z.B. Cloud-Anbieter) sind diese als Auftragnehmer häufig nicht Verantwortliche im Sinne der DS-GVO. Verantwortlich ist vielmehr in der überwiegenden Mehrzahl der Fälle der Auftraggeber. Insbesondere müssen Verantwortliche auch die Anforderungen aus Art 5 Abs. 2 DS-GVO bezüglich der Rechenschaftspflicht erfüllen können. Falls Datenübermittlungen in Drittländer an Auftragsverarbeiter erfolgen, sind auch die Bedingungen des Art. 28 DS-GVO (hier insb. Abs. 1 und

3) einschlägig, um die Nachweise nach Art. 5 Abs. 2 DS-GVO erfüllen zu können. Daher muss Lesern der Anwendungshinweise zum Data Privacy Framework klar sein, dass die Hinweise für Datenexporteure in Kap. II , Kasten am Ende von Abschnitt 2.1 so verstanden werden müssen, dass aufgrund der fehlenden Regelungen des Data Privacy Frameworks zu datenschutzrechtlichen Verpflichtungen der DS-GVO der Verantwortliche diese im Zweifel ohne Hilfe des Datenexporteurs erfüllen können muss, oder diese über einen Auftragsverarbeitungsvertrag mit dem Datenimporteur nach Art. 28 DS-GVO bzw. einer Vereinbarung nach Art. 26 DS-GVO mit dem Datenimporteur sicherstellen muss. Diese Verpflichtungen von Verantwortlichen wären z.B. Betroffenenrechte wie das Recht auf Auskunft oder das Recht auf Löschung oder das Recht auf Berichtigung. Insoweit kann ein Datenexporteur (Verantwortlicher) sich bei der Unterstützung zur Wahrung der Nutzerrechte auch nur auf vertragliche Zusicherungen des Datenimporteurs (Auftragsverarbeiter) verlassen. Technische Vereinbarungen zu Verarbeitungszwecken, auch im Rahmen der im DPF-Zertifikat benannten Verarbeitungszwecke, sowie technische Sicherheitsmaßnahmen muss der Datenimporteur auch tatsächlich nachweisen können.

2. Kritikpunkte der Europäischen Datenschutzausschusses und von Max Schrems:
Die Zertifizierung von US-Organisationen ist immer eine Selbstzertifizierung, welche aber an einen externen Auditor ausgelagert werden kann . Die zuständige Zertifizierungsbehörde erhält einige Unterlagen aus diesem Zertifizierungsprozess , die zertifizierte Stelle muss ihre Datenschutzerklärung öffentlich zur Verfügung stellen und diese vollständig umsetzen und wird dann als „zertifizierte Stelle“ geführt. Der Wahrheitsgehalt einer Selbstzertifizierung wird erst im Beschwerdefall geprüft. Staatliche Verarbeitung von Daten (zu Zwecken der Strafverfolgung und Sicherstellung der nationalen Sicherheit) können durch Beschwerden ebenfalls überprüft werden. Für die Prüfverfahren im Beschwerdefall, aber auch für die Wahrnehmung der Betroffenenrechte laut DS-GVO, hat sowohl der Europäische Datenschutzausschuss, aber auch Max Schrems, Kritik geäußert, welche in der richterlichen Überprüfung dazu führen kann, dass der Angemessenheitsbeschluss richterlich für unwirksam erklärt wird. Max Schrems hat diesen Nachweis bereits für den Angemessenheitsbeschluss zum Privacy Shield (Rechtssache C 311/18 beim EuGH) sowie vor Inkrafttreten der DS-GVO zum Safe Harbor Abkommen (Rechtssache C-362/14 beim EuGH) erfolgreich führen können.

Die Menge an Kritikpunkten ist signifikant, weshalb der TLfDI der Auffassung ist, dass Datenexporteure, welche sich auf das Data Privacy Framework berufen wollen, sich der Kritikpunkte und damit dem Risiko des Widerrufs des Angemessenheitsbeschlusses bewusst sein sollten. Es wurde bisher folgende Kritik geäußert:

a. Europäischer Datenschutzausschuss:
Der Europäische Datenschutzausschuss (englisch EDBP) kritisierte in seiner Stellungnahme zum Entwurf des Angemessenheitsbeschlusses folgende Punkte:

- Weiterbestehende Ausnahmen für das Recht auf Auskunft von Betroffenen bleiben bestehen (laut Annex I des Angemessenheitsbeschlusses, Section III „supplemental principles“, Nr. 15, Buchstabe d insbesondere für öffentlich verfügbare Daten, aber z.B. auch für Daten zu Forschungszwecken – Details findet man in Erwägungsgrund 31 des Angemessenheitsbeschlusses und dessen Fußnote 45). D.h. die Auskunft kann verweigert werden, wenn der Datenimporteur sich z.B. hinter Daten zu Forschungszwecken „verstecken“ kann.
- Unspezifische Regelungen, wann der Anwendungsbereich des EU-US DPF überhaupt eröffnet ist. D.h. es ist unklar, wann das DPF angewendet werden kann und welche Voraussetzungen in den

Einzelfällen (z.B. bei Beschwerden, aber auch bei einer Auskunft) eigentlich erfüllt sein müssen. Annex I, Section III, Nr. 8 a ii des Angemessenheitsbeschlusses erlaubt z.B. das Recht auf Auskunft gegenüber Unternehmen ohne Vorbedingungen. Für das gleiche Recht (nur zu Zwecken der „nationalen Sicherheit“ der USA) muss laut Erwägungsgrund 178 des Angemessenheitsbeschlusses die Betroffenheit nachgewiesen werden. Gelingt dieser Nachweis in dem einen Fall nicht, wird das Privacy Framework nicht angewendet. Weiterhin gibt es Ausnahmeregelungen z.B. zu Journalisten (Annex I, Section III, Nr. 2, welche jegliche Recherchedaten vom DPF ausnehmen).

- Fehlende Definition zentraler Begriffe (und damit weiter bestehende Unklarheit bezüglich der Auslegung dieser Begriffe). Dies ist z. B. dann problematisch, wenn entschieden werden muss, ob eine Datenerfassung „verhältnismäßig“, also geeignet, erforderlich und angemessen ist. Die Begriffe werden im Angemessenheitsbeschluss und dessen Anhängen zwar durchgehend benutzt, aber nicht definiert. Damit kann jede Seite diese Begriffe unterschiedlich auslegen – und im Zweifel wird dies von den Aufsichtsstellen in den USA ausgelegt. Gleiches gilt für die Prüfung der „Notwendigkeit“ (Erforderlichkeit), aber auch der „Betroffenheit“ oder wann die Risiken für ein Individuum die Interessen der US-Organisation überwiegen (wie recht pauschal in Erwägungsgrund 31 aufgezählt).
- Fehlende Klarheit, wie Verantwortliche die Prinzipien des EU-US DPF durchsetzen sollen. Annex I Section III, Nr. 9 Buchst. d erklärt z.B. im Angestelltenverhältnis den Arbeitgeber zur primären Beschwerdestelle (und erst im Nachgang können weitere Stellen eingeschaltet werden). Weitere Anlaufstellen für Beschwerden wären je nach Beschwerdegegner das „Department of Commerce“ (DoC), das „Department of Transportation“ (DoT), die „Federal Trade Commision“ (FTC), die Datenschutzaufsichtsbehörden der EU, die zertifizierte US-Organisation, eine unklare Menge an Behörden, welche für Kriminalitätsbekämpfung zuständig sind (siehe Erwägungsgrund 107 und Fußnote 190 des Angemessenheitsbeschlusses sowie Erwägungsgrund 108 des selbigen), ein „Inspector General“, das „Privacy and Civil Liberties Oversight Board“ (PCLOB), der „Foreign Intelligence Surveillance Court“ (FISC), der „Civil Liberties Protection Officer of the Director of National Intelligence“ (ODNI CLPO) sowie der „Data Protection Review Court“ (DPRC). Die Rolle einiger Stellen wird in den Anwendungshinweisen der DSK erklärt. Die Wege zu diesen Beschwerdestellen sind ganz unterschiedlich gestaltet und für Betroffene ohne fundierte rechtliche Beratung schwer zu bewältigen.
- Vollständig fehlende Regelungen zu Profiling und zur automatisierten Entscheidungsfindung.
- Unklare Regelungen zur Massendatenerfassung für Zwecke der nationalen Sicherheit sowie deren Datenspeicherdauer und praktische Umsetzung der vereinbarten Regelungen. Hier spielt primär Erwägungsgrund 141 die Hauptrolle. Dieser erlaubt Massendatenerfassung der Geheimdienste (wie Edward Snowden 2010 offenlegte), wenn eine gezielte Datensammlung nicht möglich ist und zweitens die „Notwendigkeit“ der Maßnahme begründet werden kann. Ist dies der Fall, soll die Massendatenerfassung auf das notwendige Minimum reduziert werden. Zur Begründung der „Notwendigkeit“ und was das „notwendige Minimum“ ist, werden keine Festlegungen getroffen. Eine mit der EU-Rechtsprechung vergleichbare Auslegung ist auch hier nicht garantiert.
- Fehlende Autorisierung zur Massendatenerfassung durch eine unabhängige Stelle, sondern nur nachträgliche Prüfmöglichkeit im Fall von zugelassenen Beschwerden.
- Nachträgliche Prüfung wird nicht durchgängig durch vom Geheimdienst unabhängige Stellen gewährleistet. Vielmehr ist der hierfür eingerichtete „Foreign Intelligence Surveillance Court“ (FISC) zwar ein unabhängiges Gericht, welches jedoch an die Geheimdienste der USA angegliedert ist und dessen Tätigkeit von außen nicht weiter überprüfbar ist (siehe Annex VII des

Angemessenheitsbeschlusses) .

- Der Status der Prüfung bei einer Beschwerde gegen geheimdienstliches Handeln ist nach wie vor zu intransparent. D.h. es ist unklar, ob die Beschwerde überhaupt angenommen wurde, ob Maßnahmen getroffen wurden und welche Maßnahmen dies überhaupt sind. So wurde früher nur mitgeteilt: „Ohne zu bestätigen oder zu leugnen, dass der Beschwerdeführer Gegenstand von Aktivitäten des US-Signalnachrichtendienstes war, wurden bei der Überprüfung entweder keine erfassten Verstöße festgestellt, oder das Datenschutzüberprüfungsgericht hat eine Feststellung getroffen, die angemessene Abhilfemaßnahmen erfordert.“ In Erwägungsgrund 183 wird dieser Satz bereits als Zitat wieder aufgegriffen. Diese Mitteilung kann nun vom Betroffenen pauschal angegriffen werden, woraufhin ein ausgewählter Jurist den Beschwerdeführer vertritt.

b. Max Schrems:
Auch die gemeinnützige Organisation „NOYB – Europäisches Zentrum für digitale Rechte“, welche bereits die zurückliegenden Urteile „Schrems I“ und „Schrems II“ erwirken konnte, führt weitere Kritikpunkte auf :

- Begriff der „Verhältnismäßigkeit“ bei staatlicher Überwachung wird in den USA und in der EU unterschiedlich ausgelegt. Damit kann keine pauschale „Verhältnismäßigkeit“ oder ein Maßstab nach den Grundrechten der EU angenommen werden.
- Die Stelle des „Ombudsmannes“ wurde nun einfach nur durch mehrere Gremien, wie FTC, PCLOB oder FISC ersetzt, welche in Summe aber keine wesentlichen neuen Funktionen ausfüllen.
- Keine wesentliche Änderung von FISA Section 702. FISA Section 702 regelt die geheimdienstliche Informationsgewinnung von Nicht-US-Bürgern, welche sich wahrscheinlich außerhalb der USA aufhalten, mithilfe von dafür geeigneten elektronischen Hilfsmitteln. Darunter können auch Verfahren zur massenhaften Datenerfassung fallen, falls die Informationsgewinnung nicht anders möglich ist. Die Maßnahmen werden im Innenverhältnis der Geheimdienste genehmigt und durch geheimdienst-eigene Gerichte (wie FISC) überprüft . Diese Regelung führte u. A. in den zurückliegenden Urteilen zur Aufhebung des Angemessenheitsbeschlusses. Dazu Max Schrems: „FISA 702 muss bis Ende 2023 verlängert werden, da es im US-Gesetz eine „Verfallsklausel“ gibt. Dies wäre die perfekte Gelegenheit gewesen, das US-Gesetz zu verbessern, aber angesichts des neuen Abkommens mit der EU gibt es für die USA wenig Grund, FISA 702 zu reformieren. „

Dr. Lutz Hasse: „Unternehmen etwa sollten vor diesem Hintergrund abwägen, ob sie sensible Daten – auch Kundendaten – in die USA transferieren oder bis zur Entscheidung des EuGH vorsorglich nicht. Denn die Wahrscheinlichkeit, dass der Europäische Gerichtshof den Adäquanzbeschluss aufheben wird, ist danach recht hoch.“

Dr. Lutz Hasse Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
Häßlerstraße 8 99096 Erfurt www.tlfdi.de
