Sind aller guten Dinge drei? – Neuer Mechanismus für transatlantische Datenübermittlungen auf dem Weg…

RA Jan Spittka*

Am 25. 3. 2022 gaben die Europäische Kommission und das Weiße Haus bekannt, man habe sich auf einen neuen Mechanismus für die Übermittlung personenbezogener Daten aus der EU in die USA geeinigt. Anders als die beiden – 2015 und 2020 durch den EuGH kassierten – Vorgänger „Safe Harbor" und „EU-U.S. Privacy Shield" trägt das neue Werk mit „Trans-Atlantic Data Privacy Framework" einen deutlich technokratischeren Namen. Gewöhnen wir uns also schon einmal an die Abkürzung „TADPF", da das neue Regelwerk den datenschutzrechtlichen Diskurs im transatlantischen Rechtsraum in nächster Zeit wesentlich bestimmen wird. Vorab, bislang liegen lediglich zwei Fact Sheets vor, die den groben Rahmen des TADPF abstecken, wobei das Dokument des Weißen Hauses ein wenig mehr Details offenbart als das der Kommission. Konkrete Entwurfstexte, die man kritisch analysieren könnte, wurden bislang nicht veröffentlicht. Diese sollen im Laufe des Jahres erarbeitet werden, mit dem Ziel, Ende 2022 in Kraft zu treten.

Das TADPF dürfte keine Revolution gegenüber Safe Harbor und dem Privacy Shield werden. Wie die Vorgänger soll auch das TADPF nicht als völkerrechtliches Abkommen zwischen der EU und den USA ausgestaltet werden. Vielmehr sollen wieder auf US-Seite rechtliche Mechanismen zum Schutz von aus der EU übermittelten personenbezogenen Daten vorgesehen werden, die dann zu einem Angemessenheitsbeschluss der Kommission nach Art. 45 DSGVO für teilnehmende Organisationen (es bleibt bei dem alten Mechanismus der Selbstzertifizierung) führen sollen. Inhaltlich baut das TADPF auf dem Privacy Shield auf und scheint gezielt die Kritik des EuGH aus der Schrems II-Entscheidung (Urt. v. 16. 7. 2020 – C-311/18, K&R 2020, 588 ff.) adressieren zu wollen. Hierzu ist vorgesehen, dass durch eine neue Executive Order des US-Präsidenten (wohlgemerkt nicht durch Gesetz) der Zugang der US-Geheimdienste zu personenbezogenen Daten aus der EU auf ein erforderliches und verhältnismäßiges Maß reduziert wird. Im Fact Sheet des Weißen Hauses wird dies jedoch insoweit eingeschränkt, als nicht sämtliche Geheimdienstaktivitäten erfasst sein sollen, sondern nur „signal intelligence" (SigInt), also elektronische Aufklärung. Zudem soll ein zweistufiges Streitbeilegungssystem implementiert werden, das Europäern Rechtsschutz in den USA gewähren soll, wenn betroffene Personen der Auffassung sind, zu Unrecht in das Visier elektronischer Aufklärung durch US-Geheimdienste geraten zu sein. Zu diesem Zweck soll ein unabhängiger „Data Protection Review Court" (DPRC) geschaffen werden, der mit Personen von außerhalb der US-Regierung besetzt sein soll. Dieses Gericht soll die Kompetenz bekommen, über Ansprüche und Abhilfemaßnahmen zu entscheiden. Schließlich findet sich noch die allgemeine Formulierung, dass US-Geheimdienste Prozesse vorsehen werden, die eine effektive Aufsicht anhand neuer Standards für Datenschutz und Bürgerrechte sicherstellen sollen.

Inwieweit die neuen Maßnahmen ausreichen werden, das TADPF eine Kontrolle durch den EuGH – und hierzu wird es sicher kommen – überleben zu lassen, muss sich zeigen. Richtig ist, dass der unbeschränkte und unkontrollierte Zugang der US-Geheimdienste zu personenbezogenen Daten im Rahmen von SigInt (konkret die auf Section 702 Foreign Intelligence Surveillance Act und Executive Order 12333 gestützten Programme PRISM und UPSTREAM) der Nagel zum Sarg des Privacy Shields war. Vor allem bemängelte der EuGH den fehlenden Zugang zu unabhängiger gerichtlicher Kontrolle. Insoweit gehen eine Beschränkung der SigInt-Aktivitäten der US-Geheimdienste (so dies denn tatsächlich der Fall sein wird), gestützt durch einen möglichen effektiven Rechtsschutz vor dem DPRC in die richtige Richtung. Allerdings hat der EuGH in Schrems II auch festgehalten, dass der Prüfungsmaßstab für die Angemessenheit des Datenschutzniveaus im Drittland i. S. d. Art. 45 DSGVO die Art. 7 (Achtung des Privat- und Familienlebens) und Art. 8 (Schutz personenbezogener Daten) der Charta der Grundrechte der Europäischen Union (GRCh) sind. Ob es sich bei dem DPRC tatsächlich auch um eine unabhängige Stelle zur Überwachung des Datenschutzes i. S. d. Art. 8 Abs. 3 GRCh, vergleichbar mit einer Aufsichtsbehörde i. S. d. Art. 4 Nr. 21 DSGVO, handelt, ist jedenfalls fraglich, da Gerichte nur tätig werden können, wenn sie auch angerufen werden. Auch die weit verbreitete Kritik am Mechanismus der Selbstzertifizierung der teilnehmenden Unternehmen bleibt bestehen. Es bleibt also spannend.

* ist Rechtsanwalt und Partner in der Kanzlei Clyde & Co in Düsseldorf und auf Datenschutzrecht und Cybersecurity, insbesondere im Versicherungssektor, spezialisiert. Nach dem Studium in Münster mit Schwerpunkt im Informationsrecht war er als wiss. Mitarbeiter am ITM (zivilrechtliche Abteilung) tätig. Im Anschluss an das Referendariat, das er u. a. bei einer Datenschutzbehörde absolvierte, ist er seit 2012 als Anwalt tätig.