Datenturbulenzen statt Datenhighway: Erschüttert Trumps Kurs den transatlantischen Datenschutz?

RA Dr. Paul Voigt, Lic. en Derecho, CIPP/E*

Die Datenschutzbeziehungen zwischen der EU und den USA stehen vor einer neuen Bewährungsprobe. Das EU-U.S. Data Privacy Framework (DPF), welches Datenübermittlungen aus der EU in die USA regelt, steht vor einer ungewissen Zukunft. Sein Bestand hängt von stabilen rechtlichen Rahmenbedingungen und der konsequenten Umsetzung zugesicherter Schutzmaßnahmen in den USA ab, die so bald möglicherweise nicht mehr gegeben sind.

So steht die Executive Order 14086, die das Data Privacy Framework unterstützt, auf dem Prüfstand und möglicherweise kurz vor ihrer Aufhebung. Die Schwächung des transatlantischen Datenschutzes folgt keiner zufälligen Entwicklung, sondern fügt sich in eine strategische Agenda konservativer US-Kreise ein. Das ‚Project 2025 Playbook' skizziert, wie regulatorische Zugeständnisse an Europa zurückgenommen und US-Geheimdienste von Beschränkungen befreit werden sollen.

Auch wenn die Executive Order 14086 formell vorerst unverändert bleiben sollte, könnten die damit verbundenen Schutzmaßnahmen entwertet werden: Unter Donald Trump gewinnt die umstrittene „Unitary Executive Theory" an Einfluss – eine Verfassungsinterpretation, die dem US-Präsidenten weitreichende Kontrolle über die Bundesverwaltung zugesteht. Dadurch geraten unabhängige Behörden unter politischen Druck, was tiefgreifende Folgen für den transatlantischen Datenaustausch haben könnte.

Eine wesentliche Schutzmaßnahme des DPF ist die Einschränkung der Überwachungsmaßnahmen der US-Geheimdienste. Diese dürfen danach nur unter bestimmten Bedingungen und nach Prüfung durch den „Civil Liberties Protection Officer" (CLPO) erfolgen. Zudem sollen Eingriffe in die Privatsphäre auf das notwendige Maß beschränkt und weniger invasive Alternativen bevorzugt werden.

Verstöße gegen die dargelegten Prinzipien können EU-Betroffene von unabhängigen US-Instanzen überprüfen lassen. Der CLPO fungiert dabei als Beschwerdeinstanz und der sog. „Data Protection Review Court" (DPRC) als Rechtsmittelinstanz. Eine Schlüsselrolle spielt daneben das unabhängige „Privacy and Civil Liberties Oversight Board" (PCLOB). Es überprüft u. a., ob die Vorgaben des DPF eingehalten und Entscheidungen des CLPO und des DPRC in der Praxis auch wirklich beachtet werden.

Im Januar 2025 wurden jedoch drei PCLOB-Mitglieder, die der Demokratischen Partei angehören, aufgrund angeblicher Illoyalität entlassen. Diese Maßnahme nährt Zweifel an der Unabhängigkeit des PCLOB.

Diese Befürchtungen werden durch eine neue U.S. Executive Order vom 18. 2. 2025 weiter verstärkt. Diese regelt, dass alle Behörden – einschließlich bislang unabhängiger Regulierungsstellen – der direkten Aufsicht des Präsidenten unterliegen. Damit wächst das Risiko, dass der Schutz personenbezogener Daten unter dem DPF zwar formal fortbesteht, in der Praxis aber untergraben wird. Wenn politische Loyalität wichtiger ist als rechtsstaatliche Vorgaben und Verstöße ohne Konsequenzen bleiben, entstehen Zweifel an der Einhaltung der Datenschutzmaßnahmen.

Im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments wurden daher Forderungen laut, das DPF kritisch zu überprüfen: Bemängelt wird die politische Einflussnahme auf das Kontrollorgan PCLOB, das nach der Entlassung mehrerer Mitglieder nicht mehr beschlussfähig ist. Daneben wird in einer Anfrage moniert, dass das Department of Government Efficiency (DOGE), das unter der Leitung von Elon Musk steht, immer mehr Zugriff auf sensible staatliche Datenbanken erhält. Während die Kommission in einer Anhörung am 18. 2. 2025 noch keinen Handlungsbedarf sah, steht sie unter wachsendem Druck, in der Antwort auf die Anfrage bis spätestens 19. 3. 2025 eine klare Position zum DPF zu beziehen.

Bis auf Weiteres bleibt das Data Privacy Framework aber formal in Kraft. Solange dies der Fall ist, können sich europäische Unternehmen trotz bestehender Bedenken weiterhin auf das Framework stützen, wenn sie personenbezogene Daten in die USA übermitteln. Dies hat kürzlich auch die norwegische Datenschutzbehörde festgestellt. Sie warnt jedoch: Das Fundament des Abkommens bröckelt. Unternehmen sollten daher neben dem DPF den Rückgriff auf alternative Datentransfermechanismen, wie insbesondere die Standardvertragsklauseln, in Erwägung ziehen. (Nur) so können sie sich (einigermaßen) zukunftssicher aufzustellen.

* Dr. Paul Voigt, Lic. en Derecho, CIPP/E, ist Fachanwalt für Informations- und Technologierecht, Partner und Praxisgruppenleiter für den Bereich TMT bei Taylor Wessing. Er berät Mandanten primär zu Fragen des Datenschutz-, IT- und IT-Sicherheitsrechts.