Empfehlung der RDSK zum Umgang mit dem Angemessenheitsbeschluss für den Datenschutzrahmen zwischen der Europäischen Union und den USA

(Version 2.0 – Stand: August 2025)

Trans-Atlantic Data Privacy Framework (DPF)

Am 10. Juli 2023 hat die EU-Kommission den Angemessenheitsbeschluss für den Datenschutzrahmen zwischen der Europäischen Union und den USA angenommen. Das Trans-Atlantic Data Privacy Framework (DPF) hält fest, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die im Rahmen des DPF aus der EU an US-Unternehmen übermittelt werden. „Angemessen" meint, dass die USA ein mit dem der Europäischen Union vergleichbares Datenschutzniveau vorweisen können.

Die langfristige Sicherstellung dieses mit dem DPF erreichten Schutzniveaus ist durch die US-Politik unter Trump verbunden mit der digitalen Abhängigkeit von US-Clouddiensten jedoch akut gefährdet. Aus diesem Anlass hat die RDSK in der zweiten Version dieses Papiers ihre Empfehlungen zum Umgang mit dem aktuellen Datenschutzrahmen zwischen EU und USA angepasst (siehe Kapitel 5 bis 7).

1. Grundsätzliches

Der Europäische Gerichtshof (EuGH) hat bereits zwei Abkommen vor dem DPF (Safe Harbour, EuGH, 06.10.2015 – C-362/14 "Schrems I"; Privacy Shield, EuGH, 16.07.2020 – C-311/18 "Schrems II") für unwirksam erklärt. Mit dem neuen Abkommen soll den Bedenken des Gerichts Rechnung getragen werden, indem neue verbindliche Garantien eingeführt werden, etwa die Beschränkung des Zugriffs auf EU-Daten durch US-Geheimdienste auf ein notwendiges und verhältnismäßiges Niveau. Zudem haben die USA ein Datenschutzüberprüfungsgericht errichtet (Data Protection Review Court, DPRC), zu dem EU-Bürgerinnen und EU-Bürger Zugang haben sollen.

Eine Übermittlung von personenbezogenen Daten in Länder außerhalb der EU ist nach der Datenschutzgrundverordnung („DSGVO") nur zulässig, wenn

- ein gesetzlicher Erlaubnistatbestand erfüllt ist
  und
- weitere Voraussetzungen (der Abschluss einer Auftragsverarbeitungsvereinbarung oder eines Joint-Controller-Vertrages) gegeben sind. Hierbei ist gemäß Art. 45 ff. DSGVO sicherzustellen, dass ein angemessenes Datenschutzniveau im Empfängerland vorliegt.

Ein Transfer personenbezogener Daten in ein Drittland ist nach Art. 45 Abs. 1 DSGVO zulässig, wenn ein Angemessenheitsbeschluss bezüglich eines Drittlandes gefasst wurde.

2. Wesentliche Inhalte des DPF

Das DPF ist mithin das dritte Regelwerk für eine rechtskonforme Datenübermittlung in die USA. Bis zum Inkrafttreten des DPF am 10. Juli 2023 waren Unternehmen gehalten, andere Maßnahmen für einen Datentransfer zu ergreifen. Zumindest waren Standardvertragsklauseln („SCC“) abzuschließen, um den Schutz von personenbezogenen Daten in einem sogenannten „unsicheren Drittstaat“ sicherzustellen. Daneben waren weitere technische Maßnahmen erforderlich. Der Europäische Datenschutzausschuss (EDSA) sah beispielsweise Verschlüsselungen oder Anonymisierungen von personenbezogenen Daten vor einem Transfer für geboten an.

Das DPF soll Rechtssicherheit schaffen und Restrisiken durch folgende Neuerungen zumindest minimieren:

Die USA haben ein zweistufiges Rechtsbehelfsverfahren etabliert, in dem über Beschwerden von betroffenen Personen, deren Daten aus dem EWR an Unternehmen in den USA übermittelt wurden, geprüft werden sollen. In einem Beschwerdeverfahren können EU-Bürgerinnen und EU-Bürger eine Beschwerde beim “Civil Liberties Protection Officer” erheben. Die Beschwerde kann bei einer europäischen Datenschutzbehörde eingereicht werden. Diese gibt die Eingabe an den Officer (einem Bürgerrechtsbeauftragten der US-Nachrichtendienste) zur Prüfung weiter. In einer zweiten Stufe kann in einem Überprüfungsverfahren die Entscheidung des Officers angefochten werden. Der “Data Protection Review Court” entscheidet über die Beschwerde und kann etwa die Löschung von Daten anordnen, wenn gegen Schutzmaßnahmen verstoßen wurde.

Weiterhin haben sich die USA verpflichtet, den Zugriff auf Daten von EU-Bürgerinnen und EU-Bürger auf das zum Schutz der nationalen Sicherheit erforderliche und verhältnismäßige Maß zu beschränken.

3. Empfehlungen

Auch wenn auf der Grundlage des DPF Erleichterungen für einen Datentransfer in die USA geschaffen wurden, sollten Verantwortliche dies beachten:

a) Zertifizierungen prüfen

Das DPF entfaltet seine Wirkung nur dann, wenn der Datenimporteur, also das Unternehmen, an das personenbezogene Daten übermittelt werden, auch unter dem DPF zertifiziert ist. Der verantwortliche Datenexporteur muss mithin prüfen, ob eine entsprechende Zertifizierung besteht. Das US-Department of Commerce bearbeitet und überwacht Zertifizierungsanträge. Zertifizierungen können auf der Internetseite des Department of Commerce eingesehen werden (https://www.privacyshield.gov/list). Liegt keine Zertifizierung vor, bleibt es bei dem Stand vor Inkrafttreten des DPF einschließlich der erläuterten erforderlichen rechtlichen und technischen Sicherheitsvorkehrungen.

b) Weitere Schutzmaßnahmen ergreifen

Ein Jahr nach dem Inkrafttreten des DPF, und dann auch regelmäßig, soll von der Europäischen Kommission und den Vertretern der europäischen Datenschutzbehörden (EDSA) gemeinsam mit den zuständigen US-Behörden geprüft werden, ob die Vereinbarungen umgesetzt wurden und der neue Rechtsrahmen tatsächlich funktioniert. Ob das DPF langfristig Rechtssicherheit schafft, bleibt mithin abzuwarten, weil

- der EDSA betont hat, dass seine Zustimmung zum Abkommen vom tatsächlichen und praktischen Vollzug der von den USA getätigten Zusicherungen abhängt
  und
- bereits vor Inkrafttreten des DPF Klagen gegen das Abkommen angekündigt wurden. Dies deshalb, weil fraglich sei, ob der Civil Liberties Protection Officer (CLPO) und der sogenannte "Gerichtshof" [Data Protection Review Court] im Vergleich zum vorherigen Ombudsmann-Mechanismus des Privacy Shields den Anforderungen des Rechtes auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht genügen (Art 47 EU-GRCh), insbesondere, weil der „Gerichtshof“ nicht der Judikative, sondern der Exekutive angehört. Zudem wird bezweifelt, ob tatsächlich die Zugriffe der USA auf Daten von EU-Bürgerinnen und EU-Bürger auf das „verhältnismäßige Maß“ beschränkt sind. Die Zweifel bestehen, da die Definition der Verhältnismäßigkeit unterschiedlich vorgenommen wird: So erklärt die US Executive Order 14086 die Massenüberwachung nach FISA 702 für verhältnismäßig nach amerikanischer Auslegung. Der EuGH hat diesbezüglich eine strengere Auffassung und meint, dass die Massenüberwachung nach FISA 702 nicht „verhältnismäßig“ im Sinne des von Artikel 52 EU-GRCh ist.

Der EuGH könnte mithin nochmals einen Angemessenheitsbeschluss mit sofortiger Wirkung für ungültig erklären. Verantwortliche müssten dann umgehend reagieren. Sie sollten daher weiterhin technische Maßnahmen einsetzen, um den Schutz personenbezogener Daten vor einem Transfer in die USA zu gewährleisten.

4. Weitere Hinweise

- Das DPF ersetzt nicht den Abschluss von Auftragsverarbeitungsvereinbarungen oder Joint-Controller-Verträgen. Auf den Abschluss entsprechender Vereinbarungen ist weiterhin zu achten.
- Gemäß Art. 13 Abs. 1 lit. f) DSGVO ist der Hinweis auf einen Angemessenheitsbeschluss im Falle eines Drittlandtransfers verpflichtend. Die Datenschutzerklärungen sind entsprechend anzupassen. Bei der Angabe der Datenimporteure muss informiert werden, ob diese aufgrund einer entsprechenden Zertifizierung unter das DPF fallen.
- Die Verarbeitungsverzeichnisse nach Art. 30 DSGVO müssen aktualisiert werden und die Rechtsgrundlage dokumentieren.
- Standardvertragsklauseln behalten ihre Wirksamkeit. Sofern Zusatzgarantien an die Sicherheit der Datenübermittlung in die USA geregelt wurden, ist die Beibehaltung zu empfehlen, falls das DPF unwirksam werden sollte. Die Durchführung von Datentransfer-Folgenabschätzungen (TIAs) ist weiterhin zu empfehlen.

5. Anmerkungen zur Digitalen Abhängigkeit der Landesrundfunkanstalten von US-Clouddiensten in Bezug zur Politik unter der von Trump geführten US-Regierung 2025

Seit der Amtsübernahme durch US-Präsident Donald Trump ist fraglich, ob das durch den Angemessenheitsbeschluss zum DPF rechtlich gewährleistete Datenschutzniveau durch die USA zukünftig in der vereinbarten Form erhalten bleibt. Bereits erkennbare Schwachstellen sind folgende:

- Die Executive Order 14086, welche den Zugriff US-amerikanischer Nachrichtendienste auf EU-Daten strenger reguliert, könnte jederzeit durch Präsident Trump wieder aufgehoben werden.
- Das unabhängige Aufsichtsgremium „Privacy and Civil Liberties Oversight Board" (PCLOB), das jährlich bestätigen soll, dass US-Geheimdienste rechtskonform mit sensiblen Daten aus der EU umgehen, wurde durch die Entlassung von drei der fünf Mitglieder dieses Gremiums[1] massiv geschwächt.

Die bisherige Empfehlung, Standardvertragsklauseln (SCCs) zu vereinbaren, obwohl das DPF und Angemessenheitsbeschluss (noch) gelten, wird **nachdrücklich bekräftigt**. Ohne die Vereinbarung von SCCs besteht ein hohes Risiko eines rechtlich ungesicherten Datentransfers in die USA.

6. Digitale Souveränität – Cloud Act

Die sich ausweitende Abhängigkeit des öffentlich-rechtlichen Rundfunks von US-amerikanischen Cloud-Dienstleistern bedroht unter Berücksichtigung der genannten Risiken den Schutz sensibler personenbezogener und anderer Daten; insbesondere wegen der unberechenbaren Politik der Trump-Regierung[2] muss digitale Souveränität angestrebt werden.

Zentrale Dienste wie Microsoft Outlook sollen zukünftig ausschließlich in der Microsoft Cloud abgelegt werden. Microsoft hat kürzlich zugesichert, seine Cloud-Aktivitäten in Europa nicht einzustellen und sich auf die EU-Datengrenze für Cloud-Dienste zu stützen.

- Die EU-Datengrenze ist eine Selbstverpflichtung von Microsoft, Kundendaten und personenbezogene Daten nur innerhalb der EU und der EFTA zu speichern und zu verarbeiten. Ein Datenaustausch mit Rechenzentren außerhalb dieser Grenzen erfolgt Unternehmensangaben zufolge nicht.

Der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) von 2018 gibt den US-Behörden allerdings weitreichende Befugnisse, Daten von US-Unternehmen anzufordern, unabhängig davon, wo diese gespeichert sind.

[1] https://www.europarl.europa.eu/doceo/document/P-10-2025-000941_EN.html; https://cdt.org/insights/what-the-pclob-firings-mean-for-the-eu-us-data-privacy-framework/

[2] Trump könnte Microsoft, Apple, Google, Meta und Co anweisen europäische Daten oder Dienste, wie zum Beispiel E-Mail-Konten unzugänglich zu machen oder Drohungen dieser Art als Druckmittel zur Erreichung politischer Ziele einzusetzen. Das Microsoft nicht davor zurückschreckt, war bereits sichtbar, als Microsoft im Mai 2025 nach Trump-Sanktionen das Mail-Konto des Chefanklägers des Internationalen Gerichtshofs blockierte.

- Das heißt, selbst Daten, die in europäischen Rechenzentren gespeichert sind, können von US-Behörden angefordert werden.
- Sensible Informationen der Rundfunkanstalten könnten damit für amerikanische Behörden zugänglich sein (das betrifft unternehmensinterne Informationen oder auch Inhalte journalistischer Art).

7. Empfehlungen zur Sicherung der digitalen Souveränität:

Um die digitale Souveränität und die Datensicherheit zu sichern und um das europäische Datenschutzniveau zu erhalten, empfiehlt die RDSK den Anstalten folgende Maßnahmen:

- Aufbau einer eigenen, unabhängigen digitalen Infrastruktur
- Einsatz von Open-Source-Software – wo immer dies möglich ist
- Nutzung und Förderung europäischer Cloud-Lösungen
- Kompetenzaufbau / Investitionen in Aus- und Weiterbildung
- Zusammenarbeit mit anderen öffentlichen Einrichtungen und politische Engagement für die europäische digitale Souveränität im Hinblick auf die Sicherung der Rundfunkfreihit in Deutschland und Europa
- Ausprägung einer Hybridstrategie (europäische Clouds + On-Premise Lösungen)
- Erarbeitung von Strategien zur Rückholbarkeit von Daten
- Bereitstellung von Notfall- und Krisenmaßnahmen.

Wirksame Maßnahmen zum Aufbau und Schutz der digitalen Souveränität und damit nicht zuletzt zur Gewährleistung der Unabhängigkeit der Rundfunkanstalten muss angesichts der weltpolitischen Lage als unabdingbar angesehen werden.