Warum europäischer Datenschutz mit US-Softwareanbietern schwierig ist – Was man über das Data Privacy Framework wissen sollte

30.06.2025

Datenschutz in der EU

Die Geschichte des Datenschutzes in der EU begann maßgeblich mit der EG-Datenschutzrichtlinie 95/46/EG von 1995, die erstmals einen einheitlichen Rahmen für den Schutz personenbezogener Daten innerhalb der Europäischen Gemeinschaft schuf. Sie stellte wichtige Weichen für Transparenz, Einwilligung und Rechte der Bürgerinnen und Bürger. Die Richtlinie wurde schließlich durch die Datenschutz-Grundverordnung (DSGVO) ersetzt, welche ab 2018 europaweit geltende, einheitliche Standards etablierte, die Rechte der Bürgerinnen und Bürger deutlich stärkte und Unternehmen klare Anforderungen auferlegte.

Dank der DSGVO profitieren EU-Bürger:innen heute von einem umfassenden Schutz ihrer Privatsphäre, verbesserten Kontrollmöglichkeiten über ihre persönlichen Daten und einem einheitlichen Rechtsrahmen. Ihr räumlicher Anwendungsbereich erstreckt sich nicht nur auf in der EU ansässige Organisationen, sondern auch auf Akteure außerhalb der EU, wenn diese personenbezogene Daten von Personen in der EU verarbeiten. Das bedeutet, dass auch etwa ein US-Unternehmen ohne Niederlassung in Europa der DSGVO unterliegt, sofern es Waren oder Dienstleistungen in der EU anbietet oder das Verhalten von EU-Bürger:innen beobachtet (Art. 3 DSGVO). Durch diese weite Auslegung soll verhindert werden, dass der hohe europäische Datenschutzstandard durch Auslagerung von Datenverarbeitungen ins Ausland umgangen wird.

Drittstaaten mit angemessenem Datenschutzniveau

Um den freien Datenfluss mit Staaten außerhalb des EWR zu ermöglichen, sieht die DSGVO in Art. 45 das Instrument des Angemessenheitsbeschlusses vor. Dabei stellt die EU-Kommission nach sorgfältiger Prüfung des rechtlichen Rahmens und der tatsächlichen Praxis fest, dass ein Drittland oder eine internationale Organisation ein Datenschutzniveau bietet, das dem der EU im Wesentlichen gleichwertig ist. Ein Angemessenheitsbeschluss bedeutet nicht, dass das Datenschutzniveau identisch mit dem europäischen Recht sein muss, aber es muss hinsichtlich der Kernprinzipien und Durchsetzbarkeit „wesentlich gleichwertig" sein.

Liegt ein solcher Beschluss vor, können Unternehmen Daten legal in das betreffende Land übertragen, solange sie die übrigen DSGVO-Vorgaben einhalten. Beispiele für als „sicher" eingestufte Drittländer sind etwa Japan oder Südkorea, für die die EU-Kommission entsprechende Beschlüsse gefasst hat. Darüber hinaus existieren Angemessenheitsentscheidungen u. a. für Andorra, Argentinien, Israel, Kanada, Neuseeland, die Schweiz, Uruguay oder das Vereinigte Königreich. Wichtig ist, dass

solche Beschlüsse teilweise nicht generell gelten: So deckt z. B. der Beschluss für Kanada nur Daten ab, die unter das kanadische Datenschutzgesetz PIPEDA fallen.

Sondersituation USA - US-Gesetze als Hindernis für den Datenschutz
Die USA nehmen im Datenschutzkontext eine Sonderrolle ein, da dort kein umfassendes Bundesdatenschutzgesetz existiert. Stattdessen gibt es sektorale Regelungen und vor allem weitreichende Überwachungsgesetze, die den Behörden weitgehenden Zugriff auf Daten ermöglichen. Diese kollidieren häufig mit europäischen Datenschutzprinzipien und standen im Zentrum der Schrems-II-Entscheidung des EuGH (siehe unten). Im Einzelnen sind insbesondere folgende US-Rechtsakte relevant:

· Foreign Intelligence Surveillance Act (FISA):
Das ursprüngliche FISA-Gesetz aus dem Jahr 1978 schuf erstmals einen rechtlichen Rahmen für elektronische Überwachung zu nachrichtendienstlichen Zwecken innerhalb der USA. Durch den FISA Amendments Act von 2008 wurde das Gesetz erheblich ausgeweitet, insbesondere mit Section 702. Diese Bestimmung erlaubt US-Geheimdiensten (NSA, FBI) die gezielte, jedoch weitreichende Überwachung von Nicht-US-Bürger:innen außerhalb der USA, deren Daten über amerikanische Anbieter wie etwa Google oder Microsoft laufen. Section 702 ermöglicht somit großflächige Datenerfassungen wie beispielsweise beim PRISM-Programm, ohne dass individuelle richterliche Anordnungen erforderlich sind. Diese Praxis rückte durch die Enthüllungen von Edward Snowden im Jahr 2013 erstmals umfassend ins öffentliche Bewusstsein und sorgte international für scharfe Kritik. Section 702 gilt zwar zeitlich befristet, wurde zuletzt aber im Jahr 2024 bis mindestens April 2026 verlängert.

· Patriot Act (2001) und USA Freedom Act (2015) sowie National Security Letters (NSL)
Der Patriot Act, ursprünglich 2001 nach den Anschlägen des 11. September verabschiedet, erweitert die Befugnisse der US-Behörden massiv. In Kombination mit sogenannten National Security Letters (NSL), die keinerlei richterlicher Kontrolle unterliegen, können US-Behörden von Unternehmen personenbezogene Daten verlangen. Der 2015 verabschiedete USA Freedom Act änderte zwar einige Aspekte des Patriot Acts, etwa indem Massenerhebungen eingeschränkt wurden; dennoch bleiben umfangreiche behördliche Befugnisse bestehen. Besonders kritisch sind die National Security Letters, da sie eine Herausgabe von Daten auch ohne konkreten Verdacht und ohne vorherige richterliche Anordnung ermöglichen.

· Executive Order 12333
Diese 1981 von Ronald Reagan erlassene US-Präsidialverfügung regelt die Auslandsspionage der US-Geheimdienste. EO 12333 gilt außerhalb der USA und unterliegt nicht der Aufsicht durch Gerichte oder den US-Kongress. Sie dient den Nachrichtendiensten als Rechtsgrundlage, um weltweit („extraterritorial") Kommunikation abzufangen, selbst wenn die Daten nicht in den USA gespeichert sind. Da EO 12333 rein exekutiver Natur ist, begründet sie keinerlei einklagbare Rechte für Ausländer. Datenschutzexperten werten EO 12333 als besonders problematisch, weil sie eine massenhafte Datenerhebung im Ausland erlaubt, ohne dass die davon betroffenen EU-Bürger:innen dies erfahren oder sich wehren können.

· Cloud Act
Der Clarifying Lawful Overseas Use of Data Act verpflichtet US-Anbieter, auf Anordnung auch Daten herauszugeben, die auf ausländischen Servern liegen. Hintergrund war ein Streit zwischen Microsoft und der US-Regierung über E-Mails auf einem Server in Irland – anstatt den umständlichen Rechtshilfeweg zu gehen, schuf der US-Gesetzgeber mit dem CLOUD Act Klarheit, dass US-Gesetze für US-Unternehmen weltweit gelten. Praktisch bedeutet dies, dass z. B. Microsoft, Google oder Amazon Daten, die sie in europäischen Rechenzentren speichern, an US-Behörden aushändigen müssen, wenn ein gültiges US-Auskunftsersuchen vorlieg. Der CLOUD Act umgeht damit faktisch die geografischen Schranken: Der Speicherort in der EU schützt nicht vor US-Zugriff.

Geschichte Angleichsabkommen - Frühere Abkommen und ihre Aufhebung
Im Jahr 2000 vereinbarten die Europäische Union und die Vereinigten Staaten das sogenannte Safe-Harbor-Abkommen. Ziel war es, eine rechtliche Grundlage für den Transfer personenbezogener Daten von EU-Bürger:innen in die USA zu schaffen. Die Vereinbarung sollte gewährleisten, dass US-amerikanische Unternehmen beim Umgang mit diesen Daten Datenschutzstandards einhalten, die den europäischen vergleichbar sind.

Diese Regelung geriet jedoch spätestens 2013 durch die Enthüllungen von Edward Snowden stark in die Kritik. Snowden offenbarte weitreichende Überwachungsprogramme der US-amerikanischen Geheimdienste, die auch Daten von EU-Bürger:innen betrafen. Diese Enthüllungen führten zu erheblichen Zweifeln an der tatsächlichen Einhaltung der vereinbarten Datenschutzstandards.

Als Konsequenz erklärte der Europäische Gerichtshof (EuGH) im Oktober 2015 das Safe-Harbour-Abkommen für ungültig (Schrems I). Hintergrund war eine Klage des österreichischen Datenschutzexperten Max Schrems, der argumentierte, dass die USA aufgrund der dortigen Überwachungspraktiken kein angemessenes Datenschutzniveau gewährleisten könnten.

Nach dieser Entscheidung handelten die EU-Kommission und die US-Regierung unter Präsident Barack Obama ein neues Abkommen namens Privacy Shield aus. Im Juli 2016 beschloss die EU-Kommission dieses Abkommen, welches erneut den transatlantischen Datenaustausch absichern sollte.

Doch auch das Privacy-Shield-Abkommen hielt den Prüfungen vor dem EuGH nicht stand. Im Juli 2020 entschied der EuGH im sogenannten Schrems-II-Urteil, dass auch diese Nachfolgeregelung ungültig sei. Die Richter stellten fest, dass weiterhin keine ausreichenden Schutzmechanismen gegen den Zugriff von US-Geheimdiensten auf europäische Daten gewährleistet wurden.

Das EU-U.S. Data Privacy Framework (DPF) von 2023
Im Anschluss an die Ungültigkeitserklärung des EuGH signalisierte die EU-Kommission unter Ursula von der Leyen und die Biden-Administration, dass sie daran interessiert sind, schnell eine politische Lösung in Form eines dritten Abkommens auf den Weg zu bringen. Im Juli 2023 trat das EU-U.S. Data Privacy Framework durch den Angemessenheitsbeschluss der EU Kommission in Kraft.

Ähnlich wie bei Safe Harbor/Privacy Shield wird der Datentransfer nur US-Unternehmen gestattet, die vom Handelsministerium eine Zertifizierung erhalten haben bzw. diese regelmäßig verlängern. Sie verpflichten sich, freiwillig bestimmte Datengrundsätze einzuhalten. Die beim Privacy Shield bemängelte Beschwerdestelle wird durch einen umfangreicheren Beschwerdemechanismus ersetzt. Erstmals verwendet die amerikanische Seite die Formulierungen Notwendigkeit und Verhältnismäßigkeit. Auf die beiden neuen Aspekte gehen wir weiter unten ein.

Die von amerikanischer Seite als Ergänzung zu den Regelungen des vorherigen Privacy Shield Abkommens eingebrachten Regelungen wurden allesamt durch die Executive Order 14086 - ein Präsidialerlass von Präsident Biden aus dem Jahr 2022 geschaffen. Die 'Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities' und die auf ihr basierenden nachgelagerten Behördenerlässe waren somit die Basis des Data Privacy Frameworks.

Gesetzliche Änderungen seit dem Privacy Shield Abschluss
In den USA gelten weiterhin die Gesetze rund um FISA und die Executive Order 12333. Die Verlängerung relevanter Abschnitte in FISA fand erst 2024 erneut statt und gilt mindestens bis April 2026. Neu dazugekommen ist der Cloud Act 2018. Da das Gesetz erst später in Kraft trat, spielte es im Schrems-II Urteil keine Rolle. Eine Erstbewertung durch die europäische Datenschutzbehörde fand erst 2019 statt, sie fällt wenig überraschend sehr kritisch aus. Die gesetzliche Grundlage für eine europarechtssichere Lösung ist also noch schwieriger geworden.

Verhältnismäßigkeit - Section 2 EO 14086
Da der EuGH die Formulierung "Signals intelligence activities shall be as tailored as feasible." („Nachrichtendienstliche Überwachungsmaßnahmen sollen möglichst präzise erfolgen") aus der Presidential Policy Directive -- Signals Intelligence Activities (PPD-28 von 2014) im Schrems-II Urteil als unzureichend eingestuft hat, verwendet die US-Administration bei der Anforderungsbeschreibung der Verhältnismäßigkeit in Section 2 der Executive Order die Formulierungen aus Artikel 52 der Charta der Grundrechte der Europäischen Union "necessary" und "proportionate".

Allerdings wird in der Section 2 auch gleich klargestellt, dass Massenüberwachung nicht ausgeschlossen ist und diese Executive Order keine Einschränkung der nachrichtendienstlichen Erhebungstechniken aus FISA und der Executive Order 12333 darstellt. Die Worte bei der Formulierung, welche Geheimdiensttätigkeit verhältnismäßig ist und was als notwendig gilt, sind also in der EU und den USA erstmal gleich, allerdings werden die Begriffe unterschiedlich definiert.

Beschwerdemechanismus im DPF - Section 3 EO 14086
Im Schrems-II-Urteil beanstandete der EuGH ausdrücklich die fehlenden Rechtsbehelfe und Kontrollmechanismen bei Überwachungsmaßnahmen auf Basis von FISA 702 und EO 12333.

Section 3 der Executive Order 14086 etabliert nun einen verbindlichen, zweistufigen Rechtsbehelfsmechanismus für EU-Bürger:innen, die vermuten, von US-Nachrichtendiensten im Rahmen von Signalaufklärungsmaßnahmen betroffen zu sein:

• Civil Liberties Protection Officer (CLPO)
EU-Bürger:innen müssen sich an ihre nationale Datenschutzbehörde wenden, welche eine Beschwerde an den CLPO weiterleitet. Der CLPO prüft eingehende Beschwerden und stellt anhand definierter Kriterien fest, ob es sich um ein „qualifying complaint" handelt. Die betroffene Person erhält als Antwort auf die Beschwerde entweder die Auskunft, dass kein Verstoß festgestellt wurde oder, dass ein Verstoß festgestellt wurde und die US-Regierung angemessene Maßnahmen zur Behebung ergriffen hat. Ob die Person von US-Überwachungsmaßnahmen betroffen war, wird in der Auskunft weder bestätigt noch dementiert. Der CLPO ist beim Office of the Director of National Intelligence (ODNI) angesiedelt – der Behörde unter Leitung der Direktorin der nationalen Nachrichtendienste.

· Data Protection Review Court (DPRC)
Wird die Entscheidung des CLPO nicht akzeptiert, kann die Person aus der EU, die Beschwerde eingelegt hatte – ebenso wie ein Nachrichtendienst selbst – eine Überprüfung beim Data Protection Review Court beantragen. Ein dreiköpfiges Gremium verhandelt dabei geheim, ob der CLPO rechtlich korrekt entschieden hat. Die Person aus der EU, die Beschwerde eingelegt hat, wird dabei durch einen „Special Advocate" vertreten, der von der Justizministerin ernannt wird. Auch bei einem Verfahren vor dem DPRC erhalten EU-Bürger:innen die gleiche Auskunft wie bereits im Verfahren beim CLPO. Das Gremium untersteht dem Justizministerium und wird in Absprache mit dem Handelsministerium, der Direktion der nationalen Nachrichtendienste und des PCLOB besetzt.

· Aufsichtsgremium: Privacy and Civil Liberties Oversight Board (PCLOB)
Das bereits bestehende PCLOB erhält die zusätzliche Aufgabe, den Mechanismus zu überwachen. Es prüft sowohl die Funktionsweise des CLPO wie auch des DPRC, bewertet deren Einhaltung gesetzlicher Vorgaben und empfiehlt gegebenenfalls Anpassungen. Einmal jährlich wird ein Bericht veröffentlicht. Das Gremium besteht aus fünf Personen, darunter ist eine Person für den Vorsitz vorgesehen. Alle Mitglieder werden auf Vorschlag des US-Präsidenten besetzt.

Rechtliche Fragilität durch US-Gesetze und Tricks der Exekutive Order
Es handelt sich bei dem Data Privacy Framework um ein rechtlich fragiles Konstrukt. Die US-Gesetzeslage hat sich nicht verbessert, sondern ist mit dem Cloud-Act noch schwieriger als vorher geworden. Der Cloud-Act führt sogar dazu, dass die von US-Cloud-Anbietern vermarktete sogenannte Datenhaltung in der EU oder Datenresidenz EU - die bereits aus technischer Sicht etwa wegen fehlender echter

Kontrolle über Zugangsmöglichkeiten keine Verbesserung darstellt - auch rechtlich eindeutig untergraben wird.

Datenschutzexperten wie Max Schrems weisen darauf hin, dass die unterschiedliche Definition von Verhältnismäßigkeit auf beiden Seiten des Atlantiks juristisch nicht haltbar ist. In der Praxis ist keine Gleichwertigkeit bei der Prüfung von Überwachungsmaßnahmen gegeben. Er weist außerdem darauf hin, dass der als Beschwerdemechanismus betitelte Prozess, der EU-Bürger:innen ihre Rechte sichern soll, vor allem kosmetischer Natur ist. Ein Gericht wird nicht dadurch ein Gericht, indem man ein Exekutivgremium als solches bezeichnet.

Erschwerend kommt hinzu, dass der Beschwerde-Mechanismus nicht darauf ausgelegt zu sein scheint, dass man ihn benutzt. EU-Bürger:innen können nur auf Verdacht hin eine Beschwerde einreichen, da sie über mögliche Überwachungsmaßnahmen nicht informiert werden – eine Benachrichtigungspflicht existiert nicht. Das Verfahren beginnt beim Civil Liberties Protection Officer (CLPO), dessen Entscheidung nicht offenlegt, ob tatsächlich eine Überwachung stattgefunden hat. Das heißt im Umkehrschluss auch, dass EU-Bürger:innen die Entscheidung beim DPRC anfechten können, aber gar nicht mitteilen können, weshalb sie das tun, da die entsprechende Information nicht erteilt wurde. Das Ergebnis eines Verfahrens vor dem DPRC wiederum gibt auch keine Auskunft darüber, ob die Person von US-Geheimdiensten überwacht wurde oder wird.

Nach dem letzten Bericht des PCLOB gab es noch keine einzige Beschwerde - trotz zuletzt (2022) knapp 250.000 nach section 702 überwachten Personen die nicht die US-Staatsbürgerschaft besitzen. Zu anderen gesetzlichen Grundlagen außer Section 702 gibt es gar keine Zahlen. Es erscheint unrealistisch, dass die USA nicht massenhaft EU-Bürger:innen überwacht, die nach EU-Recht vor solcher Überwachung geschützt wären.

Fragilität durch Exekutiv-Konstruktion
Wie bereits an mehreren Stellen erwähnt, basiert das komplette Data-Privacy-Framework nur auf einem Exekutiverlass und den darauf basierenden nachgelagerten Behördenanordnungen.

Der Beschluss kann zu jedem Zeitpunkt innerhalb einer Sekunde hinfällig werden. Es reicht dafür eine Unterschrift von US-Präsident Donald Trump. Auch können einzelne Rechtsbehelfsgremien jederzeit von der Justizministerin, der Direktorin der nationalen Nachrichtendienste oder eben des Präsidenten in ihrer Zusammensetzung verändert, in ihren Möglichkeiten eingeschränkt oder aufgelöst werden.

Wie groß die Macht der Exekutive ist, zeigt sich an der Aushöhlung des PCLOB. Donald Trump entfernte im Januar 2025 die demokratischen Mitglieder des PCLOB, welches folglich kein Quorum mehr für Entscheidungen hatte. Dadurch, dass auch die Vorsitzende durch Trump entfernt wurde ist das Gremium nach seinen eigenen Statuten nicht handlungsfähig, da es sich nur beim Vorsitz um eine Vollzeitstelle handelt, welche auch die Befugnis zur Anstellung von Personal hat. Während zwei

demokratische Mitglieder im Mai nach einem Gerichtsbeschluss wieder eingesetzt wurden, war die Amtszeit der Vorsitzenden bereits abgelaufen, sodass das Gremium weiterhin geschwächt ist - wie bereits in Trumps erster Amtszeit, als es allerdings noch kein Data Privacy Framework gab.

Darüber hinaus können präsidiale Erlässe die ohnehin schon fragwürdige Konstruktion weiter destabilisieren. Ein Beispiel hierfür ist die von Donald Trump im Februar 2025 erlassene Executive Order 14215, die beispielsweise die Unabhängigkeit der Federal Trade Commission (FTC) bei der Durchsetzung der DPF-Prinzipien beeinträchtigen könnte.

Ebenfalls ein konkretes Beispiel ist die Executive Order 14203, der die Sperrung des Outlook-Accounts des Chefanklägers am Internationalen Strafgerichtshof Karim Khan zur Folge hatte. Hier zeigt sich, dass Firmen wie Microsoft umgehend auf die Präsidialverfügungen reagieren müssen und keine Datenresidenzen und sonstige Mechanismen EU-Bürger:innen vor den Exekutiverlässen des US-Präsidenten schützen.

Juristisches Prüfverfahren
Die europäischen Gerichte können - wie schon die vorherigen beiden Abkommen - auch dieses für nicht angemessen erklären. Die Verfahren dazu laufen bereits. Der französische Abgeordnete Philippe Latombe reichte 2023 Klage ein. Eine Anhörung vor dem Gerichtshof der Europäischen Union fand am 1.April 2025 statt. Ein Urteil könnte noch in diesem Jahr folgen. Ein dritter Rückschlag in Folge vor der EU-Rechtsprechung dürfte das Ende der Bemühungen um solche Abkommen bedeuten - auch angesichts der Tatsache, dass die Kommission ein gesetzliches Entgegenkommen der USA benötigen würden und mit der Trump-Administration verhandeln müsste. Unternehmen und Organisationen, die sich für diesen Fall absichern wollen, sollten sich jetzt umsehen, welche Software von europäischen Firmen bezogen oder welche Open Source Software durch europäische Firmen bereitgestellt werden kann.

Quellen:

https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (Angemessenheitsbeschlüsse)
https://www.activemind.legal/guides/adequacy-decision (Angemessenheitsbeschlüsse)
https://de.wikipedia.org/wiki/CLOUD_Act (Cloud Act)
https://www.dr-datenschutz.de/das-us-datenschutzniveau-als-problem-beim-cloud-computing/ (Cloud Act)
https://de.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act (FISA)
https://noyb.eu/en/eu-us-data-transfers-0 (EU US Data Transfer - NOYB)
https://www.taylorwessing.com/de/insights-and-events/insights/2025/01/eu-us-data-privacy-frameworks (Data Privacy Framework)
https://www.edps.europa.eu/sites/default/files/publication/19-07-10_edpb_edps_cloudact_annex_en.pdf (Cloud Act EDPS)
https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities (EO14086)
https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (PPD-28)
https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court (DPRC)
https://www.politico.com/news/2024/01/17/inside-bidens-secret-surveillance-court-00136175 (Beschwerdemechanismus in der Praxis)
https://kpmg-law.de/zweifel-an-us-praesident-bidens-executive-order-zum-datenschutz/ (EO14086)
https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu (Data Privacy Framework - NOYB)
https://www.retarus.com/blog/de/privacy-shield-standardvertragsklauseln-cloud-act-was-datenschuetzer-max-schrems-verunsicherten-unternehmen-nun-raet/ (NSL)
https://www.pogo.org/analysis/executive-order-12333-the-spy-power-too-big-for-any-legal-limits (EO 12333)
https://documents.pclob.gov/prod/Documents/EventsAndPress/6e6c7a7b-6036-4d6d-b635-ffb53f68e4f4/Statement%20on%20PCLOB%20Review%20Under%20Section%203%20of%20EO%201408 6%2C%20Completed%20508%2C%20Nov%207%202024.pdf (PCLOB Report redress mechanism)
https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-855706216063/2023%20PCLOB%20702%20Report%20%28002%29.pdf (No. targeted non-US-citizens 2022 - section 702)
https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752 (Questions & Answers: EU-US Data Privacy Framework)
https://www.lewissilkin.com/insights/2025/03/30/could-trump-play-the-trump-card-against-the-data-protection-framework-102k26v (EO 14215 - consequences)
https://public-inspection.federalregister.gov/2025-03063.pdf (EO 14215)
https://www.hoganlovells.com/en/publications/latombe-case-first-hearing-for-annulment-of-the-euus-data-privacy-framework (Latombe Case)