ChatGPT

Datenverarbeitung in EU-Rechenzentren von US-Anbietern: DSGVO-Konformität 2024/25

Hintergrund: EU-Datenschutz vs. US CLOUD Act

Die DSGVO verlangt, dass personenbezogene Daten nur dann in Drittländer übertragen oder dort verarbeitet werden dürfen, wenn ein angemessenes Schutzniveau gewährleistet ist (Art. 44 ff. DSGVO). **US-Gesetze wie der CLOUD Act erschweren dies erheblich:** Der *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)* von 2018 verpflichtet alle US-Unternehmen – und sogar deren ausländische Tochterfirmen – zur Herausgabe von Daten an US-Behörden, **unabhängig vom Speicherort** [1]. Das bedeutet: Selbst wenn Daten physisch in einem Rechenzentrum innerhalb der EU liegen, kann ein US-Anbieter (z. B. Amazon, Microsoft, Google) per US-Recht gezwungen werden, diese an amerikanische Behörden auszuhändigen [1]. Dies geschieht oft **ohne Wissen der Betroffenen oder europäischer Stellen** und potentiell im Widerspruch zur DSGVO [2].

Ein **aktuelles Beispiel** verdeutlicht das Problem: In einer Anhörung vor dem französischen Senat 2022 räumte der Justiziar von Microsoft Frankreich ein, dass Microsoft *nicht garantieren kann*, dass Daten europäischer Behörden nicht an die US-Regierung weitergegeben werden – man müsse gültigen US-Anordnungen kooperativ nachkommen [3]. **Ähnlich hat Amazon (AWS)** erklärt, man könnte theoretisch ebenfalls verpflichtet werden, EU-Daten an US-Stellen zu geben (auch wenn dies bisher nicht vorgekommen sei und man sich nach Kräften wehren würde) [4]. Diese Aussagen unterstreichen, dass **US-Anbieter die Hoheit über in der EU gespeicherte Daten abgeben müssen**, sobald US-Behörden anklopfen – eine klare Spannungslage zwischen EU-Datenschutz und US-Rechtsordnung.

EU-Rechenzentren allein genügen nicht: Manche US-Cloudanbieter werben mit "EU Regions" oder einem *„EU Data Boundary"* (z. B. rein europäische Rechenzentren und Admin-Teams) als Lösung. **Doch Aufsichtsbehörden warnen, dass solche Maßnahmen keinen vollständigen Schutz bieten** [5]. Die verwendete Software stammt meist aus den USA, und der Anbieter unterliegt dem CLOUD Act – *latente Zugriffsmöglichkeiten* (etwa via Remote-Zugriff durch US-Personal) bleiben bestehen [5]. Diese sind technisch kaum überprüfbar, sodass selbst deutsche Datenschutzbehörden keine effektive Kontrolle über einen möglichen US-Zugriff haben [5]. **Fazit:** Auch wenn die Daten in Europa lagern, kann ein US-Anbieter aufgrund der Rechtslage in den USA nicht garantieren, dass europäische Datenschutzstandards eingehalten werden.

Schrems II-Urteil und Folgen für Datentransfers

Im Juli 2020 fällte der Europäische Gerichtshof das wegweisende *Schrems II*-Urteil (Rechtssache C-311/18). Darin wurde der EU–US **Privacy Shield** (ein Angemessenheitsabkommen) für ungültig erklärt, **weil US-Überwachungsgesetze wie FISA 702 und der CLOUD Act EU-Bürgern kein mit der EU vergleichbares Datenschutzniveau bieten** [6] [7]. Die Richter betonten, dass umfangreiche Zugriffsbefugnisse von US-Behörden und fehlende Rechtsschutzmöglichkeiten für EU-Betroffene mit der DSGVO unvereinbar sind [6]. Zwar blieben die EU-Standardvertragsklauseln (*Standard Contractual Clauses*, SCCs) als Transferinstrument gültig, **jedoch nur unter der Bedingung**, dass der Datenexporteur **zusätzlich prüft und sicherstellt**, dass im Empfängerland ein *„im Wesentlichen gleichwertiges"* Schutzniveau herrscht [6]. Praktisch bedeutet das: Unternehmen müssen für

Datentransfers in die USA **Fall-zu-Fall-Risikobewertungen (Transfer Impact Assessments)** durchführen und ggf. **zusätzliche Schutzmaßnahmen** ergreifen, um DSGVO-Konformität zu gewährleisten.

Die Schrems-II-Entscheidung schlug hohe Wellen bei Aufsichtsbehörden in der EU. Viele **Datenschutzbehörden verschärften ihre Haltung** gegenüber US-Diensten. Beispielsweise erklärte die österreichische Datenschutzbehörde 2022 die Nutzung von Google Analytics (mit Serverkontakt in den USA) für rechtswidrig. Ähnliche Entscheidungen trafen Aufsichtsbehörden in **Frankreich, Italien und anderen Ländern**, die den Einsatz bestimmter US-Online-Dienste wegen der Zugriffsmöglichkeiten durch US-Stellen untersagten [8]. In Deutschland äußerten die Datenschutzbehörden ebenfalls Bedenken: **Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK)** stellte Ende 2022 fest, dass eine Nutzung von Microsoft 365 **ohne Übermittlung personenbezogener Daten in die USA nicht möglich ist** [9]. Mit anderen Worten: Öffentliche Stellen wie Schulen können nach Ansicht der DSK *nicht sicherstellen*, dass Schülerdaten bei Einsatz von MS365 ausreichend geschützt sind [9].

Sogar Gerichte haben diese Linie bestätigt. So entschied die Vergabekammer Baden-Württemberg im Juli 2022, **dass der Einsatz von US-Cloud-Anbietern wegen Art. 44 ff. DSGVO rechtswidrig ist** [10]. Die Begründung folgt der Logik von Schrems II: Solange US-Geheimdienste Zugriff auf die Daten nehmen können, ist das erforderliche Datenschutzniveau nicht gegeben [10]. Unternehmen wie Meta/Facebook gerieten ebenfalls unter Druck – im Mai 2023 verhängte die irische Datenschutzbehörde (koordiniert durch den EDSA) ein Rekordbußgeld von 1,2 Mrd. € gegen Meta und verpflichtete das Unternehmen, **alle EU-Nutzerdaten zurück in EU-Rechenzentren zu holen**, weil Meta unter US-Überwachungsgesetzen wie FISA 702 Daten in die USA übermittelt hatte [6]. Max Schrems kommentierte, dass im Grunde **jeder große US-Cloud-Anbieter** (Amazon, Google, Microsoft etc.) von ähnlichen Maßnahmen betroffen sein könnte, solange die US-Gesetze keinen besseren Schutz für EU-Daten bieten [8].

Die **praktische Konsequenz** aus Schrems II: **Datenübermittlungen in die USA sind nur noch zulässig, wenn zusätzliche Garantien greifen**. In vielen Fällen kamen Aufsichtsbehörden zum Schluss, dass **wirksame technische Schutzmaßnahmen kaum umsetzbar sind** – etwa bei komplexen Cloud-Diensten, wo selbst Verschlüsselung nicht alle personenbezogenen Daten vor dem Zugriff schützen kann [11]. Der Europäische Datenschutzausschuss (EDSA) betonte 2023, dass öffentliche Stellen notfalls **auf EU-souveräne Cloud-Lösungen ausweichen** müssen, wenn kein gleichwertiger Schutz durch US-Anbieter erreicht werden kann [11]. Insgesamt herrschte bis 2023 große Rechtsunsicherheit: Viele Unternehmen verharrten in einem *„Cloud-Dilemma“*, da weder die Nutzung US-basierter Services sicher datenschutzkonform möglich schien, noch gleichwertige europäische Alternativen stets verfügbar waren.

Aktuelle Entwicklungen: EU-US Data Privacy Framework (Angemessenheitsbeschluss)

Um den Transatlantik-Datenverkehr auf eine neue Grundlage zu stellen, haben EU und USA 2023 das **EU–US Data Privacy Framework (DPF)** eingeführt. Die Biden-Regierung erließ hierzu *Executive Order 14086*, die bestimmte Beschränkungen für US-Geheimdienste und ein neues Beschwerdeverfahren für EU-Bürger vorsieht [12]. Auf dieser Basis hat die EU-Kommission im Juli 2023 einen **Angemessenheitsbeschluss** getroffen [13]: Zertifizierte US-Unternehmen gelten demnach wieder als sichere Empfänger für EU-Daten. **Mit dem Data Privacy Framework können personenbezogene Daten an teilnehmende US-Anbieter übertragen werden, ohne dass weitere Garantien (wie SCCs) nötig sind**, weil die USA für diese Unternehmen als „angemessenes“

Datenschutz-Niveau anerkannt wird. Große Cloud-Anbieter wie AWS, Microsoft und Google haben sich umgehend nach Inkrafttreten des DPF zertifizieren lassen [14], um ihren EU-Kunden Rechtssicherheit zu bieten.

Unterschied Standardvertragsklauseln vs. DPF: Standardvertragsklauseln bleiben weiterhin gültige Instrumente, aber sie erfordern nach Schrems II **zusätzliche Prüf- und Schutzmaßnahmen**. Bei SCCs verpflichtet sich der Datenimporteur zwar vertraglich zur DSGVO-Einhaltung, doch **das Risiko durch entgegenstehendes US-Recht (CLOUD Act, FISA) bleibt** bestehen. Daher müssen Exporteure *im Einzelfall* beurteilen, ob der US-Anbieter die vertraglichen Zusicherungen überhaupt einhalten kann – und ggf. **technische Maßnahmen** (Verschlüsselung, Pseudonymisierung) ergänzen [15]. Das DPF hingegen **schafft einen allgemeineren Rahmen**: US-Unternehmen, die sich den DPF-Prinzipien unterwerfen, profitieren von einem pauschalen Angemessenheitsstatus, **ohne dass der EU-Datenexporteur selbst eine umfangreiche Transferprüfung durchführen muss**. In der Praxis vereinfacht dies den Einsatz von US-Cloud-Diensten deutlich, **solange** sich der Anbieter an die DPF-Auflagen hält (z.B. Löschungspflichten, begrenzte Weitergabe, Kooperation mit dem neuen Datenschutz-Gerichtshof in den USA bei Beschwerden).

Allerdings ist zu beachten, dass das Data Privacy Framework **bereits kontrovers diskutiert** wird. Datenschutzexperten und sogar das EU-Parlament übten Kritik, dass die USA durch das DPF **noch nicht vollständig ein „Schutzniveau im Sinne der DSGVO" erreicht** haben [16]. Max Schrems und seine Organisation *noyb* haben angekündigt, das DPF juristisch überprüfen zu lassen. Zudem ist die *politische Stabilität* des Abkommens nicht garantiert: Sollte z. B. eine zukünftige US-Regierung (Donald Trump hat es bereits angekündigt) die neue Executive Order wieder aufheben oder abschwächen, **fiele die Grundlage des Angemessenheitsbeschlusses weg** [17]. In diesem Fall stünde man erneut vor einem Schrems-II-Szenario. **Unternehmen müssen sich also bewusst sein**, dass das DPF zwar aktuell gültig ist, aber möglicherweise nicht dauerhaft Bestand hat – eine Phase erhöhter Rechtsunsicherheit ist einkalkuliert [18].

Einschätzung der Aufsichtsbehörden in der EU (2024/2025)

Derzeit vertreten europäische Datenschutzaufsichtsbehörden eine vorsichtige bis kritische Linie bezüglich US-Cloud-Anbietern unter dem CLOUD Act. Die **deutschen Behörden** betonen, dass auch nach Einführung des DPF die Risiken nicht vom Tisch sind. So warnt der Bundesbeauftragte für den Datenschutz (BfDI) vor einem *„Blindflug"*, wenn Unternehmen allein auf Zusicherungen der Anbieter vertrauen – die tatsächliche Kontrolle über die Daten bleibe problematisch. Die **Datenschutzkonferenz (DSK)** hat bislang keine Entwarnung gegeben: Bis Microsoft oder andere US-Firmen wirksame Nachbesserungen nachweisen, bleibt z.B. der Einsatz von Diensten wie Microsoft 365 in vielen Behörden untersagt oder nur mit strengen Auflagen geduldet [9]. Auch andere nationale Behörden halten an ihren **Untersagungsverfügungen** fest (z.B. bezüglich Google Analytics oder Facebook Connect), solange kein belastbarer Schutz vor US-Zugriffen besteht [8].

Gleichzeitig erkennen die Aufsichtsbehörden an, dass das **EU-US Data Privacy Framework** einen Schritt in die richtige Richtung darstellt. Die französische CNIL und andere haben Infos veröffentlicht, wie Unternehmen das DPF nutzen können. Dennoch raten viele Behörden: **Sich nicht ausschließlich darauf verlassen!** Vielmehr sollen Firmen **vorsorglich Standardvertragsklauseln und zusätzliche Maßnahmen bereit halten**, falls das DPF scheitert oder ein spezieller Dienst nicht unter das DPF fällt [19]. Der Europäische Datenschutzausschuss (EDSA) hat das DPF zwar grundsätzlich begrüßt, aber ebenfalls **nachbesserungswürdige Punkte** identifiziert (u.a. bei den Kriterien für Verhältnismäßigkeit von Überwachung) [20] [21]. Bis zur ersten jährlichen Überprüfung des DPF (voraussichtlich 2024) bleiben die Behörden daher aufmerksam.

In Summe lautet die *aktuelle Auffassung*: **Eine DSGVO-konforme Verarbeitung personenbezogener Daten in EU-Rechenzentren durch US-Anbieter ist möglich, aber an strenge Bedingungen geknüpft.** Ohne entsprechende Garantien (Angemessenheitsbeschluss oder wirksame zusätzliche Schutzmaßnahmen) sehen Aufsichtsbehörden in der Regel **keine Rechtsgrundlage** für solche Transfers – im Zweifel gilt die Verarbeitung als unzulässig [10] [8]. Mit geeigneten Vorkehrungen hingegen kann das Risiko beherrschbar gemacht werden, was im nächsten Abschnitt erläutert wird.

Praxisempfehlungen für Unternehmen

Unternehmen, die Cloud-Dienste von US-Anbietern nutzen möchten, sollten **proaktiv Maßnahmen ergreifen**, um DSGVO-Konformität sicherzustellen. Basierend auf den aktuellen Leitlinien der Behörden lassen sich folgende Empfehlungen aussprechen:

- **Teilnahme am Data Privacy Framework prüfen:** Nutzen Sie bevorzugt US-Anbieter, die nach dem **EU-US DPF** zertifiziert sind. Ist Ihr Cloud-Dienstleister auf der Liste der zertifizierten Unternehmen, gilt der Datentransfer (vorerst) als zulässig und bedarf keiner weiteren Genehmigung [13]. *Dennoch* sollten Sie die Entwicklung beobachten, da das DPF politisch und juristisch anfällig ist [17].

- **Standardvertragsklauseln abschließen:** In jedem Fall (auch ergänzend zum DPF) empfiehlt sich der Abschluss der **neuen Standardvertragsklauseln** mit dem Anbieter. Diese modernen SCCs (seit 2021) enthalten umfangreiche Verpflichtungen des US-Anbieters, etwa Informierungspflichten bei behördlichen Anfragen. Wichtig: Verlangen Sie vom Cloud-Anbieter **Transparenz**, ob und wie oft Behörden Daten angefordert haben. Vertragsklauseln alleine genügen aber nicht – es kommt auf die praktische Umsetzung an.

- **Transfer Impact Assessment (Risikoanalyse):** Führen Sie eine **Drittland-Risikoabwägung** durch, in der Sie dokumentieren, welche Daten verarbeitet werden, welche Zugriffsrisiken durch US-Recht bestehen und welche Schutzmaßnahmen Sie ergreifen. Berücksichtigen Sie dabei, dass allgemeine (nicht sensible) Daten zwar ein geringeres Risiko darstellen mögen als Gesundheits- oder Finanzdaten, *aber* auch hier ein Grundrechtseingriff vorliegt, falls US-Behörden unberechtigt zugreifen. **Legen Sie die Ergebnisse der Datenschutzbehörde auf Nachfrage vor**, um Ihre Compliance zu belegen.

- **Technische Schutzmaßnahmen einsetzen:** Wo immer möglich, sollten **technische Vorkehrungen** getroffen werden, um den Zugriff durch Unbefugte (und damit auch durch US-Stellen) auszuschließen. Praxisnahe Maßnahmen sind z.B.:

- **Verschlüsselung:** Speichern Sie personenbezogene Daten **client-seitig verschlüsselt**, sodass der Cloud-Anbieter selbst keinen Klartext sieht. Die Schlüsselverwaltung sollte in Europa bleiben (idealerweise inhouse beim Kunden). Somit könnte ein US-Anbieter selbst bei einem CLOUD-Act-Erzwingungsbeschluss nur chiffrierte Daten herausgeben, die für Behörden unbrauchbar sind – **das reduziert das Risiko erheblich** [15].
- **Pseudonymisierung und Minimierung:** Gestalten Sie die Daten so, dass der Cloud-Dienst *keine direkten Personenbezüge* enthält, wo immer es der Zweck erlaubt. Wenn z.B. Identifikationsmerkmale durch Codes ersetzt werden, die nur Ihr Unternehmen auflösen kann, sind *im Fall eines Datenzugriffs keine personenbezogenen Informationen erkennbar*. Zudem gilt das Prinzip der **Datenminimierung**: Laden Sie nur jene Daten in die Cloud, die für die Verarbeitung unbedingt nötig sind.

- **„EU-only"-Optionen nutzen:** Einige Anbieter bieten Konfigurationen an, um Support-Zugriffe auf EU-Personal zu beschränken oder Daten in bestimmten Regionen zu halten. Nutzen Sie solche Optionen (z.B. *Microsoft EU Data Boundary* ab 2023) und dokumentieren Sie sie. *Beachten Sie jedoch*, dass dies kein vollumfänglicher Schutz ist – wie oben erläutert, bleibt ein Restrisiko [5]. Deshalb sollten EU-only Maßnahmen **immer kombiniert mit Verschlüsselung/ Pseudonymisierung** eingesetzt werden.

- **Überwachung und Logging:** Etablieren Sie Verfahren, um Zugriffe auf Ihre Cloud-Daten zu protokollieren. Verdächtige Zugriffsereignisse (etwa durch Admin-Accounts aus dem Ausland) können so erkannt und dem Anbieter hinterfragt werden. 100%igen Schutz bietet das zwar nicht, aber es erhöht die Chance, unautorisierte Zugriffe festzustellen.

- **Europäische Alternativen evaluieren:** Langfristig lohnt es sich, **digitale Souveränität zu stärken** [22]. Prüfen Sie, ob es **europäische Cloud-Anbieter** gibt, die Ihre Anforderungen erfüllen. Diese unterliegen nicht dem US-Recht, was das Compliance-Risiko drastisch senkt. Auch hybride Ansätze sind möglich: Hochkritische personenbezogene Daten bleiben in einer EU-Cloud oder on-premise, während weniger sensible Workloads bei einem US-Hyperscaler laufen. So reduzieren Sie die Abhängigkeit und das Risiko (*Prinzip der Risikostreuung*).

- **Notfallplan bereit halten:** Entwickeln Sie für den Fall neuer rechtlicher Entwicklungen einen Plan B. Sollte z.B. der Angemessenheitsbeschluss (DPF) durch Gerichte gekippt werden, müssen Sie **rasch auf SCCs + zusätzliche Maßnahmen umschalten** können [19]. Halten Sie Ihre Verträge und Assessments aktuell, und beobachten Sie News aus EU-Rechtsprechung und US-Gesetzgebung. So vermeiden Sie, von einem plötzlichen Wegfall der Rechtsgrundlage überrascht zu werden.

Fazit

Zusammenfassend lässt sich festhalten, dass die Verarbeitung *nicht-sensibler personenbezogener Daten* in EU-Rechenzentren von US-Anbietern **nur unter bestimmten Bedingungen DSGVO-konform sein kann**. Entscheidend ist, ob ein Schutzniveau wie in der EU sichergestellt wird. Der neue **EU-US Data Privacy Framework** bietet hierfür einen aktuellen (wenn auch politisch unsicheren) Weg, indem er zertifizierten US-Unternehmen ein *„angemessenes"* Datenschutzniveau attestiert [13]. **Alternativ** können weiterhin Standardvertragsklauseln genutzt werden – dann jedoch **mit ergänzenden technischen Vorkehrungen**, um die Risiken durch den US CLOUD Act abzupuffern [15]. In jedem Fall erwarten die europäischen Aufsichtsbehörden, dass Unternehmen **größte Sorgfalt walten lassen**, den Einzelfall prüfen und notfalls auf Anbieter wechseln, die uneingeschränkt der DSGVO unterliegen [11].

Unter **Einhaltung dieser Voraussetzungen** ist die Nutzung von AWS, Azure, Google Cloud & Co. *prinzipiell möglich*. Unternehmen müssen jedoch jederzeit gewährleisten können, dass **kein unbefugter Drittländer-Zugriff** erfolgt bzw. dass die Rechte der Betroffenen gewahrt bleiben. Gelingt dies – etwa durch DPF-Zertifizierung oder wirksame Verschlüsselung – steht einer DSGVO-konformen Verarbeitung in der Cloud nichts im Wege. **Ohne solche Sicherungen** läuft man hingegen Gefahr, dass die Verarbeitung **nicht DSGVO-konform** ist und von Behörden untersagt oder sanktioniert wird [10] [8]. Die aktuelle Tendenz ist klar: *Datenschutzbehörden gehen im Zweifel lieber auf Nummer sicher* – deshalb sollten das auch die Unternehmen tun, indem sie ihre Cloud-Datenschutzstrategien an die neuesten Anforderungen anpassen.

---

1 5 12 13 17 18 19 22 Datentransfer in die USA: Neue Risiken durch Trumps Kurswechsel
https://exkulpa.de/datenschutz/datentransfer-in-die-usa-neue-risiken-durch-trumps-kurswechsel/

2 3 US law in European data centres? The CLOUD Act makes it possible | OpenCloud
https://opencloud.eu/en/the-cloud-act-makes-it-possible

4 Amazon’s new European Sovereign Cloud - a strategic response to US Law and EU Data Privacy - DEV Community
https://dev.to/aws-builders/amazons-new-european-sovereign-cloud-a-strategic-response-to-us-law-and-eu-data-privacy-ed3

6 7 8 16 € 1.2 Mrd Rekordstrafe wegen Metas EU-US Datentransfers
https://noyb.eu/de/edsa-entscheidung-zu-facebooks-datenuebertragung-die-usa

9 Hintergrund: Beschluss der Datenschutzkonferenz vom 24.11.2022 zu Microsoft 365 - Bayerischer Elternverband e.V.
https://www.bev.de/digitalisierung/dsk-ueber-ms365

10 15 Cloud Anbieter in den USA rechtswidrig: Zum Beschluss der Vergabekammer Baden-Württemberg - Dr. DSGVO
https://dr-dsgvo.de/cloud-anbieter-in-den-usa-rechtswidrig-zum-beschluss-der-vergabekammer-baden-wuerttemberg/

11 edpb.europa.eu
https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf

14 The EU-U.S. Data Privacy Framework - Amazon Web Services (AWS)
https://aws.amazon.com/compliance/eu-us-data-privacy-framework/

20 Adequate for now: EDPB's opinion on the level of data protection in ...
https://technologyquotient.freshfields.com/post/102lw5e/adequate-for-now-edpbs-opinion-on-the-level-of-data-protection-in-the-uk

21 EDPB issues Its Opinion on the EU-U.S. Data Privacy Framework
https://www.hunton.com/privacy-and-information-security-law/edpb-issues-its-opinion-on-the-eu-u-s-data-privacy-framework