punkt.exe
PUNKTEXE RESEARCH

WHITEPAPER · JULI 2026
STAND 03.07.2026 · V1.1

EU-US DATA PRIVACY FRAMEWORK · TRUMP V. SLAUGHTER · DSGVO KAP. V

TRANSFER UNTER VORBEHALT.

Ein Urteil in Washington stellt die Rechtsgrundlage des transatlantischen Datenverkehrs infrage. Was das für deutsche Unternehmen bedeutet, welche Fristen jetzt laufen und wie Sie Architekturen bauen, die regulatorische Schocks überleben.

29.06.2026 · SCOTUS 6:3

TRUMP V. SLAUGHTER, NO. 25-332: FTC-UNABHÄNGIGKEIT VERFASSUNGSWIDRIG

259×

VERWEISE AUF DIE FTC IM EU-ANGEMESSENHEITSBESCHLUSS (EU) 2023/1795

3. Anlauf

NACH SAFE HARBOR (†2015) UND PRIVACY SHIELD (†2020) WACKELT NUN DAS DPF

WAS SIE AUF DEN FOLGENDEN SEITEN ERWARTEN

AKT I · DAS URTEIL

AKT II · DIE RISIKOLAGE

AKT III · DIE ANTWORT

WERKZEUG & ANHANG

WENIG ZEIT? Geschäftsführung: S. 03, 10, 20 · IT & Sicherheit: Kap. 08–09 · Recht & Datenschutz: Kap. 01–07

HINWEIS ZUR EINORDNUNG

Dieses Whitepaper wurde am 3. Juli 2026 abgeschlossen, vier Tage nach dem Urteil des US Supreme Court. Die Lage entwickelt sich weiter. Alle rechtlichen Aussagen dienen der Information und ersetzen keine Rechtsberatung im Einzelfall. Aussagen, die als „Punktexe-Einschätzung" gekennzeichnet sind, sind begründete Bewertungen, keine Prognosen.

DAS WICHTIGSTE AUF EINER SEITE

Am 29. Juni 2026 hat der US Supreme Court die gesetzlich verankerte Unabhängigkeit der Federal Trade Commission für verfassungswidrig erklärt. Genau diese Unabhängigkeit war eine tragende Annahme des EU-US Data Privacy Framework, der wichtigsten Rechtsgrundlage für Datentransfers in die USA.

6:3

MEHRHEIT IM SUPREME COURT. GEKIPPT WIRD EIN PRÄZEDENZFALL VON 1935 (HUMPHREY'S EXECUTOR)

259×

STÜTZT SICH DER EU-ANGEMESSENHEITSBESCHLUSS AUF DIE FTC ALS UNABHÄNGIGE AUFSICHT

2–3 Jahre

DAUERT EIN EUGH-VERFAHREN ERFAHRUNGSGEMÄSS. DIE LATOMBE-BERUFUNG LÄUFT BEREITS SEIT OKT. 2025

01 NICHTS IST HEUTE VERBOTEN. ABER DIE BEGRÜNDUNG IST WEG.

Der Angemessenheitsbeschluss bleibt formal in Kraft, bis die EU-Kommission ihn aufhebt oder der EuGH ihn für nichtig erklärt. Es gibt keine automatischen Bußgelder und keine Pflicht, morgen den Stecker zu ziehen. Aber die tragende Argumentation des Beschlusses, eine unabhängige US-Aufsicht, existiert seit dem 29. Juni nicht mehr.

02 SCC-NUTZER SIND SOFORT IN DER PFLICHT, NICHT ERST „WENN ES KIPPT".

Wer Transfers auf Standardvertragsklauseln oder Binding Corporate Rules stützt, muss sein Transfer Impact Assessment jetzt aktualisieren. Diese Bewertungen verweisen üblicherweise auf FTC, PCLOB und Data Protection Review Court als unabhängige Kontrollinstanzen. Alle drei Annahmen sind nach der Urteilslogik hinfällig.

03 KI-SYSTEME VERVIELFACHEN DIE EXPONIERUNG.

Prompts, RAG-Kontexte, Agenten-Logs und Meeting-Mitschnitte sind personenbezogene Datenflüsse in Echtzeit. Wer Copilot, ChatGPT oder US-gehostete Modelle einsetzt, hat mehr Transfers als sein Verfahrensverzeichnis vermuten lässt.

04 WIRKSAM SIND FAST NUR TECHNISCHE MASSNAHMEN.

Der Europäische Datenschutzausschuss hält rein vertragliche und organisatorische Zusatzmaßnahmen für unzureichend. Was trägt: Verschlüsselung mit Schlüsselhoheit in der EU, Pseudonymisierung vor dem Transfer, Confidential Computing, Gateway-Architekturen mit austauschbaren Modellen.

05 DIE PLANUNGSANNAHME LAUTET: 12 BIS 24 MONATE VORBEREITUNGSFENSTER.

Kurzfristig kippt nichts. Mittelfristig ist ein „Schrems III" realistisch. Wer jetzt inventarisiert, klassifiziert und Schlüsselhoheit aufbaut, handelt aus Stärke. Wer wartet, handelt später unter Zeitdruck, zu Krisenkonditionen.

> **Die eigentliche Frage ist nicht, ob Sie US-Technologie nutzen. Die Frage ist, ob ein Gerichtsurteil in Washington Ihr Unternehmen stoppen kann.**

EIN URTEIL IN WASHINGTON. FOLGEN IN EUROPA.

Trump v. Slaughter liest sich wie ein innenpolitischer Verfassungsstreit über Präsidentenmacht. Tatsächlich trifft die Entscheidung den tragenden Pfeiler, auf dem ein erheblicher Teil der europäischen Cloud- und KI-Nutzung rechtlich ruht.

WAS AM 29. JUNI ENTSCHIEDEN WURDE

Mit 6:3 Stimmen hat der US Supreme Court in der Rechtssache Trump v. Slaughter (No. 25-332) entschieden, dass der gesetzliche Entlassungsschutz für Kommissionsmitglieder der Federal Trade Commission verfassungswidrig ist.[1]

Auslöser war die Entlassung der demokratischen FTC-Kommissare Rebecca Slaughter und Alvaro Bedoya im Frühjahr 2025, zu Beginn der zweiten Amtszeit von Präsident Trump. Beide wurden ohne die gesetzlich vorgesehenen Gründe wie Dienstvergehen oder Pflichtverletzung entlassen. Die Vorinstanzen hatten die Entlassungen noch als rechtswidrig eingestuft. Der Supreme Court sah es anders und gab der Regierung recht.[4][11]

1.1 EIN PRÄZEDENZFALL VON 1935 FÄLLT

Die Entscheidung verwirft Humphrey's Executor v. United States aus dem Jahr 1935. Seit gut neun Jahrzehnten galt: Der Kongress darf Mitglieder unabhängiger Aufsichtsbehörden mit Kündigungsschutz ausstatten, eine Absetzung ist nur aus wichtigem Grund („for cause") möglich. Diese Konstruktion schützte die FTC und rund zwei Dutzend weitere Behörden vor direktem politischem Durchgriff.[4][12] Einzig für die Federal Reserve formulierte das Gericht ausdrücklich eine Ausnahme.[1]

1.2 DIE BEGRÜNDUNG: UNITARY EXECUTIVE THEORY

Die konservative Mehrheit folgt der sogenannten Unitary Executive Theory. Nach dieser Verfassungslesart muss der Präsident die uneingeschränkte Kontrolle über alle Exekutivbehörden besitzen. Gesetzliche Regelungen, die einzelne Behörden vor dem direkten Durchgriff des Präsidenten schützen, sind demnach verfassungswidrig.[4]

WARUM DAS KEIN REINES US-THEMA IST

Die Logik des Urteils beschränkt sich nicht auf die FTC. Sie erfasst strukturell jede US-Exekutivstelle, deren Unabhängigkeit bisher gesetzlich oder per Verordnung abgesichert war. Damit trifft sie exakt die Bausteine, mit denen die USA gegenüber der EU ein „gleichwertiges Datenschutzniveau" belegt haben: unabhängige Aufsicht und unabhängiger Rechtsschutz.

1.3 DIE UNMITTELBARE REAKTION

Noch in der Nacht nach dem Urteil forderte die Datenschutzorganisation noyb um Max Schrems die EU-Kommission in einem formellen Schreiben auf, den Angemessenheitsbeschluss für die USA in einem geordneten Verfahren aufzuheben. Die Begründung: Nach dem Urteil gebe es in den USA schlicht keine unabhängigen Aufsichtsbehörden mehr, auf die sich die EU stützen könne. Eine Nichtigkeitsklage wurde für die kommenden Wochen angekündigt.[3]

Aus dem Europäischen Parlament kamen erste politische Reaktionen: Das Datenschutzabkommen sei kollabiert, die Kommission müsse aktiv werden, die Antwort liege in europäischer digitaler Souveränität.[13] Die Kommission selbst hat sich zum Redaktionsschluss dieses Papiers nicht formell positioniert; ein Sprecher kündigte lediglich an zu prüfen, ob das Urteil die Gültigkeit des DPF berührt. Beobachter erwarten, dass sie sich Zeit lässt: Ein schneller Rückzug aus dem Abkommen gilt als politisch und wirtschaftlich kaum vorstellbar.[14]

DIE TRANSATLANTISCHE KETTE: WARUM DIE FTC DAS DPF TRÄGT

Um zu verstehen, warum ein US-Verfassungsurteil europäisches Datenschutzrecht trifft, muss man die Kette kennen, an der der transatlantische Datenverkehr hängt. Sie hat fünf Glieder. Das Urteil durchtrennt zwei davon.

NR	GLIED	FUNKTION
1	**Art. 44 ff. DSGVO**	Personenbezogene Daten dürfen nur in Drittländer, wenn das Schutzniveau dort „der Sache nach gleichwertig" ist. Grundsatz seit 1995.
2	**Art. 45 DSGVO: Angemessenheitsbeschluss**	Die EU-Kommission kann per Beschluss feststellen, dass ein Drittland angemessenen Schutz bietet. Dann fließen Daten ohne weitere Instrumente.
3	**Durchführungsbeschluss (EU) 2023/1795**	Der aktuelle Beschluss für die USA, in Kraft seit 10. Juli 2023: das EU-US Data Privacy Framework (DPF).[2]
4	**Unabhängige Aufsicht: die FTC**	EU-Primärrecht (Art. 16 Abs. 2 AEUV, Art. 8 Abs. 3 GRCh) verlangt zwingend eine unabhängige Datenschutzaufsicht. Diese Rolle übernimmt in den USA die FTC. Der Beschluss verweist nach Zählung von noyb 259-mal auf sie.[3][4]
5	**Rechtsschutz: EO 14086, DPRC, PCLOB**	Executive Order 14086 (2022) begrenzt Geheimdienstzugriffe, schafft den Data Protection Review Court (DPRC) und stützt sich auf die Aufsicht des Privacy and Civil Liberties Oversight Board (PCLOB).[2][12]

2.1 GLIED 4 IST GERISSEN

Die FTC untersteht nach dem Urteil der direkten Weisungsbefugnis des Präsidenten. Die Unabhängigkeit, auf die sich die Kommission in ihrem Beschluss 259-mal beruft, ist damit als tragende Annahme entfallen. Andere im Beschluss genannte Stellen, etwa das Department of Transportation, haben keine vergleichbare Durchsetzungsfunktion und unterliegen als Exekutivbehörden derselben Urteilslogik.[12]

2.2 GLIED 5 WAR SCHON VORHER BESCHÄDIGT

Der DPRC ist kein Gericht im Sinne von Art. 47 der EU-Grundrechtecharta, sondern eine Stelle innerhalb des US-Justizministeriums. Seine Unabhängigkeit beruht ausschließlich auf einer präsidialen Anordnung, die jederzeit widerrufbar ist. Diese Kritik ist nicht neu: Schon 2023 stellte das Europäische Parlament fest, dass der DPRC den Anforderungen des Art. 47 GRCh an Unabhängigkeit und Unparteilichkeit nicht genügt.[31][32] Das PCLOB ist seit der Entlassung dreier Mitglieder im Januar 2025 ohne Quorum und kann seine Aufsichtsfunktion nur eingeschränkt wahrnehmen.[9][12][33]

> **EU-Primärrecht fordert unabhängige Aufsicht. Die US-Verfassung verbietet sie nach neuer Lesart. Dieser Widerspruch lässt sich weder durch Wahlen noch durch Zusagen einzelner Konzerne auflösen.**

Auflösbar wäre der Konflikt nur durch eine einstimmige Änderung der EU-Verträge oder eine Neuausrichtung des US-Verfassungsrechts. Beides ist auf absehbare Zeit nicht in Sicht.[12]

MUSTER MIT ANSAGE: ZWEIMAL GEKIPPT, EINMAL WACKLIG

Die aktuelle Lage ist kein Betriebsunfall. Sie ist die dritte Wiederholung desselben Konflikts: EU-Grundrechtsschutz trifft auf US-Überwachungsrecht. Zweimal hat der EuGH bereits entschieden. Beide Male gegen das Abkommen.

● 2000–2015
SAFE HARBOR
Gekippt am 6.10.2015 durch Schrems I (EuGH, C-362/14). Kernproblem: US-Massenüberwachung, fehlender Rechtsschutz.

● 2016–2020
PRIVACY SHIELD
Gekippt am 16.7.2020 durch Schrems II (EuGH, C-311/18). Kernproblem: FISA 702, EO 12333, kein wirksamer Rechtsbehelf.

● 2023–?
DATA PRIVACY FRAMEWORK
In Kraft seit 10.7.2023. EuG-Klage abgewiesen (9/2025), Berufung beim EuGH anhängig, seit 29.6.2026 ohne tragende Begründung.

○ 2027+
„SCHREMS III"?
Latombe-Berufung und angekündigte noyb-Klage machen eine dritte EuGH-Entscheidung zum realistischen Szenario.

3.1 DAS STRUKTURELLE PROBLEM BLEIBT DASSELBE

Beide Vorgänger scheiterten an identischen Hürden: Section 702 des Foreign Intelligence Surveillance Act und Executive Order 12333 erlauben US-Diensten weitreichende Zugriffe auf Daten von Nicht-US-Bürgern, ohne dass diese über einen gleichwertigen Rechtsbehelf verfügen. Der 2018 hinzugekommene CLOUD Act verpflichtet US-Anbieter zur Herausgabe von Daten unter ihrer Kontrolle, unabhängig vom Speicherort.[6][15]

Das DPF sollte diese Kritik über die Executive Order 14086 entschärfen: Verhältnismäßigkeitsprinzip für die Datenerhebung, Beschwerdeweg über den DPRC, Aufsicht durch das PCLOB. Der Konstruktionsfehler: Alles Wesentliche beruht auf exekutiven Zusagen statt auf parlamentarischem Gesetz. Genau diese Fragilität materialisiert sich seit 2025 Stück für Stück: PCLOB gelähmt, DPRC-Unabhängigkeit infrage gestellt, FTC-Unabhängigkeit gekippt.[7][12]

3.2 WAS DIESMAL ANDERS IST

Schrems I und II handelten von Überwachungsbefugnissen, also davon, was US-Recht **erlaubt**. Trump v. Slaughter handelt davon, was US-Verfassungsrecht **verbietet**: nämlich genau die Art unabhängiger Aufsicht, die das EU-Recht zwingend voraussetzt. Damit ist der Konflikt, solange diese Verfassungsrechtsprechung steht, erstmals nicht politisch verhandelbar. Kein viertes Abkommen kann eine Behörde unabhängig machen, deren Unabhängigkeit das oberste US-Gericht für verfassungswidrig erklärt hat.

FORMAL GÜLTIG. MATERIELL ENTKERNT.

Das Data Privacy Framework gilt weiter, und genau das macht die Lage tückisch: Es gibt keinen Alarm, keine Frist, keine Abmahnung im Briefkasten. Nur eine Rechtsgrundlage, deren Begründung nicht mehr existiert, und drei Verfahrenswege, auf denen sie fallen kann.

DREI WEGE, AUF DENEN DAS DPF FALLEN KANN

Der Angemessenheitsbeschluss verschwindet nicht von selbst. Er bleibt wirksam, bis ihn die Kommission widerruft oder der EuGH ihn für nichtig erklärt. Solange er gilt, sind auch die Aufsichtsbehörden an ihn gebunden und dürfen für DPF-gestützte Transfers keine Bußgelder verhängen.[16] Entscheidend ist deshalb, welche Verfahren jetzt laufen und wie schnell sie sind.

4.1 WEG 1: DIE KOMMISSION WIDERRUFT SELBST

noyb hat die Kommission formell zum geordneten Rückzug aufgefordert.[3] Politisch gilt dieser Weg als unwahrscheinlich: Ein Widerruf würde den transatlantischen Datenverkehr über Nacht auf Ausnahmetatbestände und Standardvertragsklauseln zurückwerfen, mitten in einem ohnehin angespannten Handelsverhältnis. Realistischer ist, dass die Kommission das Urteil im Rahmen ihrer laufenden Überprüfungspflicht bewertet und auf Zeit spielt.[14]

4.2 WEG 2: DIE LATOMBE-BERUFUNG (LÄUFT BEREITS)

Der französische Abgeordnete Philippe Latombe hatte den Beschluss vor dem Gericht der EU angefochten. Das EuG wies die Klage am 3. September 2025 ab (T-553/23), prüfte dabei aber ausdrücklich nur die Sach- und Rechtslage zum Zeitpunkt des Beschlusses im Juli 2023. Das weicht vom bisherigen EuGH-Maßstab ab, wonach der Zeitpunkt der gerichtlichen Prüfung zählt.[5][12] Das Rechtsmittel ist seit dem 31. Oktober 2025 unter dem Aktenzeichen C-703/25 P beim EuGH anhängig. Es kann genau diesen Punkt angreifen, und Trump v. Slaughter liefert dem Gerichtshof dafür frisches, kaum ignorierbares Material. Rechtsmittelverfahren dauerten zuletzt im Schnitt 18,4 Monate (EuGH-Jahresstatistik 2024); eine Entscheidung ist damit ab 2027 denkbar.[12][17][34]

BEMERKENSWERT: MICROSOFT TRITT DEM VERFAHREN BEI

Am 28. Juni 2026, einen Tag vor dem Supreme-Court-Urteil, gab Microsoft bekannt, dass der Gerichtshof das Unternehmen als Streithelfer auf Seiten der Kommission im Latombe-Verfahren zugelassen hat.[8] Das Interesse ist legitim und offen benannt: Es geht um die Rechtsgrundlage eines wesentlichen Teils des eigenen Geschäftsmodells. Juristisch löst der Beitritt das Kernproblem aber nicht. Ob das US-Recht „wesentlich gleichwertigen" Schutz bietet, entscheidet sich an der US-Rechtsordnung, nicht am Verhalten einzelner Anbieter.[12]

4.3 WEG 3: DIE ANGEKÜNDIGTE NOYB-KLAGE („SCHREMS III")

noyb will in den kommenden Wochen eine eigene Nichtigkeitsklage gegen den Beschluss einreichen; sie beginnt formal vor dem Gericht der EU (EuG). Solche Verfahren dauern über die Instanzen erfahrungsgemäß zwei bis drei Jahre.[3][11] Die Organisation hat mit Safe Harbor und Privacy Shield bereits zwei Abkommen vor dem EuGH zu Fall gebracht. Ihr zentrales Argument ist diesmal einfacher als je zuvor: Das EU-Recht verlangt unabhängige Aufsicht, und die gibt es in den USA nach höchstrichterlicher Feststellung nicht mehr.

> **Beide gerichtlichen Wege enden vor demselben Gerichtshof, der bereits zweimal gegen ein solches Abkommen entschieden hat. Der dritte Weg hängt am politischen Willen der Kommission.**

SZENARIEN UND ZEITHORIZONTE: DIE PUNKTEXE-EINSCHÄTZUNG

Niemand kann ein Gerichtsurteil vorhersagen, auch wir nicht. Was sich seriös bewerten lässt: die Stärke der Argumente, die Dauer der Verfahren und die Konsequenzen je Szenario. Genau darauf sollte Ihre Planung aufbauen.

SZENARIO	BESCHREIBUNG	ZEITHORIZONT	EINSCHÄTZUNG
A · Zähe Kontinuität	Kommission wartet ab, Verfahren ziehen sich, DPF bleibt formal in Kraft. Rechtsunsicherheit und Sorgfaltspflichten steigen kontinuierlich.	2026–2028	Kurzfristig das wahrscheinlichste Szenario
B · „Schrems III"	EuGH kippt den Beschluss (Latombe-Berufung ab 2027 möglich, noyb-Klage eher 2028/29). Übergangsfrist ungewiss, bei Schrems II gab es keine.	2027–2029	Realistisch; Eintrittsrisiko deutlich gestiegen
C · Geordneter Rückzug	Die Kommission widerruft selbst und verhandelt Übergangsregeln. Juristisch sauber, politisch teuer.	offen	Unwahrscheinlich ohne äußeren Zwang
D · Politische Eskalation	Datentransfers werden Verhandlungsmasse im Handelskonflikt; abrupte Verschärfungen auf einer der beiden Seiten.	jederzeit	Restrisiko, nicht planbar, aber absicherbar

5.1 DIE PLANUNGSANNAHME

Für die Unternehmensplanung folgt daraus eine klare Arbeitsgrundlage: **Behandeln Sie das DPF als gültige, aber endliche Rechtsgrundlage.** Als formales Transferinstrument lebt es. Als Planungsgrundlage für Architekturentscheidungen mit mehrjähriger Laufzeit ist es ungeeignet. Das Vorbereitungsfenster, in dem Sie aus eigener Kraft handeln können, beträgt nach unserer Einschätzung 12 bis 24 Monate.

5.2 WARUM WARTEN TEUER WIRD

Bei Schrems II entfiel der Privacy Shield am Tag der Urteilsverkündung, ohne Übergangsfrist. Unternehmen mussten binnen Wochen auf SCC umstellen und Zusatzmaßnahmen improvisieren. Wer damals vorbereitet war, unterschrieb Nachträge. Wer nicht vorbereitet war, verhandelte unter Zeitdruck mit Anbietern, die tausende identische Anfragen gleichzeitig bearbeiteten. Migrationsprojekte aus der Not heraus kosten erfahrungsgemäß ein Mehrfaches geplanter Vorhaben, bei sechs bis achtzehn Monaten realistischer Wechseldauer je Workload.

5.3 WAS GEGEN DEN ALARM SPRICHT

Die Gegenposition verdient Ernsthaftigkeit, denn sie hat drei valide Argumente: Das EuG hat die Klage gegen das DPF 2025 in erster Instanz abgewiesen. Die Kommission kann nachsteuern, etwa indem sie der US-Seite Nachbesserungen abringt. Und keiner Aufsichtsbehörde ist daran gelegen, die eigene Wirtschaft über Nacht ins Unrecht zu setzen; einige Kanzleien raten entsprechend zu Ruhe statt Aktionismus.

Nur: Alle drei Argumente betreffen das Tempo, nicht die Richtung. Sie verlängern das Vorbereitungsfenster, sie schließen es nicht. Und keines von ihnen repariert den Kern, dass die tragende Annahme des Beschlusses entfallen ist. Genau deshalb lautet die Planungsannahme dieses Papiers 12 bis 24 Monate, und nicht null.

PUNKTEXE-EINSCHÄTZUNG IN EINEM SATZ

Kurzfristig kippt nichts, mittelfristig ist ein erneutes Scheitern vor dem EuGH das realistische Basisrisiko, und die einzige Variable, die Sie kontrollieren, ist Ihr eigener Vorbereitungsgrad.

BETROFFENHEIT: WER EXPONIERT IST UND WARUM KI ALLES VERSCHÄRFT

Betroffen ist praktisch jedes Unternehmen, das personenbezogene Daten über US-Dienste verarbeitet. Also: E-Mail und Kollaboration (Microsoft 365, Google Workspace), CRM und Marketing (Salesforce, HubSpot), Infrastruktur (AWS, Azure, Google Cloud) und KI-Dienste (OpenAI, Anthropic, Copilot, Gemini).

6.1 DREI GRUPPEN, DREI DRINGLICHKEITEN

DPF-Nutzer: formal weiter legal. Aber die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) verlangt, die neue Lage zu bewerten und einen Plan B zu dokumentieren. Unter NIS2 kommt die Risikomanagementpflicht hinzu.[19]

SCC- und BCR-Nutzer: sofortiger Handlungsbedarf. Ihre Transfer Impact Assessments stützen sich üblicherweise auf FTC, PCLOB und DPRC als unabhängige Instanzen. Diese Annahmen sind hinfällig; die Bewertungen müssen unverzüglich aktualisiert werden.[9][11]

Regulierte Branchen: Finanzdienstleister, Gesundheitswesen, KRITIS-Betreiber und der öffentliche Sektor tragen verschärfte Nachweispflichten und Reputationsrisiken. Für sie ist der dokumentierte Notfallplan keine Kür.[10]

6.2 DER KI-FAKTOR: TRANSFERS, DIE IM VERFAHRENSVERZEICHNIS FEHLEN

Klassische Transfer-Inventuren denken in Datenbanken und Dateiablagen. KI-Systeme erzeugen dagegen personenbezogene Datenflüsse in Echtzeit: Prompts mit Kunden- und Beschäftigtendaten, RAG-Kontexte aus internen Dokumenten, Meeting-Transkripte, Agenten-Logs und persistente „Memories". Wichtig dabei: Eine „Übermittlung" im Sinne der DSGVO setzt keinen physischen Datenexport voraus. Schon der Fernzugriff aus einem Drittland genügt.[10] Wer Copilot oder US-gehostete Modelle produktiv einsetzt, hat fast immer mehr Drittlandtransfers, als das Verfahrensverzeichnis ausweist.

6.3 WAS AUCH IM ERNSTFALL WEITER GEHT

Keine Panik an zwei Stellen: Nicht-personenbezogene Daten (reine Maschinen-, Produkt- und Telemetriedaten ohne Personenbezug) sind von Kapitel V der DSGVO nicht erfasst. Und Art. 49 DSGVO erlaubt notwendige Einzeltransfers, etwa zur Vertragserfüllung: die Hotelbuchung in New York, das Ticket beim US-Support. Was Art. 49 nicht trägt, ist strukturelles Auslagern ganzer Verarbeitungen.[3]

DER SANKTIONSRAHMEN, NÜCHTERN BETRACHTET

Verstöße gegen die Übermittlungsvorschriften des Kapitels V können mit bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes geahndet werden (Art. 83 Abs. 5 DSGVO). Relevanter als Bußgelder sind in der Praxis oft Untersagungsverfügungen der Aufsicht, Audit-Findings, Vertragsverletzungen gegenüber Kunden und der Ausschluss aus Ausschreibungen mit Souveränitätsanforderungen.

VERTRÄGE BERUHIGEN. ARCHITEKTUR SCHÜTZT.

Die reflexhafte Antwort auf Transferrisiken ist juristisch: mehr Klauseln, mehr Anhänge, mehr Unterschriften. Notwendig, aber nicht hinreichend. Was im Ernstfall trägt, sind technische Maßnahmen und eine Architektur, in der Anbieter austauschbar sind.

RECHTLICHE INSTRUMENTE: SCC, TIA UND ART. 49 RICHTIG EINSETZEN

Fällt der Angemessenheitsbeschluss, wird nicht der Datenverkehr verboten. Es entfällt nur das bequemste Instrument. Die Alternativen existieren, verlangen aber echte Arbeit: Verträge plus Bewertung plus Maßnahmen.

7.1 STANDARDVERTRAGSKLAUSELN (SCC)

Die von der EU-Kommission erlassenen Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) verpflichten Datenexporteur und -importeur vertraglich auf EU-Schutzstandards. Sie sind das Auffanginstrument der Wahl. Aber seit Schrems II gilt: SCC allein genügen nicht. Der Exporteur muss prüfen, ob das Recht des Ziellandes die vertraglichen Zusagen aushebelt, und gegebenenfalls ergänzende Maßnahmen ergreifen.[6][7]

Ein Praxis-Hinweis, der Wochen sparen kann: Bei den großen US-Anbietern sind SCC häufig bereits als automatischer Fallback im Auftragsverarbeitungsvertrag verankert, etwa bei Microsoft, Google und AWS. Der erste Schritt ist deshalb keine Neuverhandlung, sondern eine Prüfung des Bestands: Greift der Fallback automatisch beim Wegfall des DPF? Für welche SCC-Module? Sind die Anhänge zu Verarbeitungsgegenstand und technisch-organisatorischen Maßnahmen vollständig ausgefüllt?

7.2 TRANSFER IMPACT ASSESSMENT (TIA)

Das TIA (auch Transfer Risk Assessment genannt) dokumentiert diese Prüfung. Der Europäische Datenschutzausschuss beschreibt dafür in seinen Empfehlungen 01/2020 ein sechsstufiges Vorgehen:[7][20]

01 **Transfers kennen:** Jede Übermittlung erfassen, auch Fernzugriffe und Weiterübermittlungen an Subdienstleister.

02 **Instrument identifizieren:** Angemessenheitsbeschluss, SCC, BCR oder Ausnahme nach Art. 49?

03 **Wirksamkeit bewerten:** Hebeln Zugriffsgesetze des Drittlandes (FISA 702, CLOUD Act) das Instrument in der Praxis aus?

04 **Zusatzmaßnahmen ergreifen:** Vorrangig technische Maßnahmen (Kapitel 08).

05 **Formale Schritte:** Verträge nachziehen, ggf. Aufsicht einbinden.

06 **Regelmäßig neu bewerten:** Bei relevanten Rechtsänderungen unverzüglich. Trump v. Slaughter ist exakt so eine Änderung.

WAS EIN TIA NACH DEM 29. JUNI 2026 ENTHALTEN MUSS

Eine ehrliche Neubewertung benennt: FTC-Unabhängigkeit höchstrichterlich verworfen, PCLOB seit Januar 2025 ohne Quorum, DPRC als Exekutivstelle auf widerruflicher Anordnungsbasis. Wer diese Fakten in seiner Bewertung übergeht, dokumentiert keine Sorgfalt, sondern deren Gegenteil, und schafft im Streitfall Beweismaterial gegen sich selbst.

7.3 BCR UND ART. 49: DIE RANDLÖSUNGEN

Binding Corporate Rules sichern konzerninterne Transfers ab, teilen aber das TIA-Problem: Auch sie schützen nicht gegen staatlichen Zugriff im Zielland. Die Ausnahmen des Art. 49 (Einwilligung, Vertragserfüllung, Rechtsansprüche) tragen notwendige Einzelfälle, taugen jedoch ausdrücklich nicht als Dauerlösung für strukturelle Datenflüsse.[3][20]

> **Juristische Instrumente verlagern das Risiko auf Papier. Ob das Papier hält, entscheidet sich an der Technik dahinter.**

TECHNISCHE MASSNAHMEN, DIE WIRKLICH TRAGEN

Der Europäische Datenschutzausschuss ist an dieser Stelle unbequem deutlich: Rein vertragliche und organisatorische Zusatzmaßnahmen schaffen für sich genommen keinen hinreichenden Schutz. Wirksam sind in aller Regel nur technische Maßnahmen, die den Zugriff auf personenbezogene Daten durch Empfänger oder Behörden im Drittland tatsächlich verhindern. [7]

8.1 DIE GRENZLINIE: KLARTEXT-ZUGRIFF

Die entscheidende Frage lautet: Kann der US-Anbieter (oder eine Behörde über ihn) auf Klartext zugreifen? Sobald der Empfänger den Klartext oder den Schlüssel besitzt, kann er zur Herausgabe verpflichtet werden, und keine Vertragsklausel der Welt ändert daran etwas.[7][21] Daraus ergibt sich eine klare Sortierung:

KONSTELLATION	BEWERTUNG NACH EDSA-LOGIK	STATUS
Backup/Storage verschlüsselt, Schlüssel ausschließlich beim EU-Exporteur	Wirksam: Der Importeur sieht nur Chiffrat, ein Behördenzugriff läuft ins Leere (EDSA Use Case 1).	TRÄGT
Pseudonymisierte Verarbeitung, Re-Identifikation nur in der EU möglich	Wirksam, wenn der Importeur den Personenbezug nicht herstellen kann und Zusatzwissen in der EU verbleibt.	TRÄGT
Transportverschlüsselung + Verschlüsselung „at rest" beim US-Anbieter mit dessen Schlüsseln	Pflichtstandard, aber gegen Behördenzugriff wirkungslos: Der Anbieter kann entschlüsseln, also kann er herausgeben.	TRÄGT NICHT
SaaS-Betrieb im Klartext (Mail, CRM, Office, KI-Assistent beim US-Anbieter)	EDSA Use Cases 6/7: Für Verarbeitung, die Klartext-Zugriff erfordert, sind keine wirksamen technischen Maßnahmen bekannt.	TRÄGT NICHT
EU-Rechenzentrum eines US-Anbieters („Datenresidenz")	Der CLOUD Act knüpft an die Kontrolle des Anbieters an, nicht an den Serverstandort. Residenz allein ist Kosmetik.[15][21]	TRÄGT NICHT

DIE UNBEQUEME KONSEQUENZ

Für einen großen Teil der heutigen US-SaaS-Nutzung existiert keine technische Maßnahme, die den Klartext-Zugriff des Anbieters verhindert und den Dienst zugleich funktionsfähig lässt. Hier hilft nur Risikosteuerung über Datenklassifikation: Was darf überhaupt hinein? Und Architektur: Wie schnell komme ich wieder heraus?

DER WERKZEUGKASTEN: ZEHN MASSNAHMEN NACH WIRKUNGSGRAD

01 Datenminimierung & Klassifikation
Die billigste Maßnahme zuerst: Was nicht übertragen wird, muss nicht geschützt werden. Ampel-Klassifikation (Kap. 09) vor jedem neuen Tool.

02 Pseudonymisierung vor dem Transfer
Direkte Identifikatoren durch Referenzen ersetzen („Kunde-924" statt Name), Zuordnungstabelle verbleibt in der EU. Vom EDSA anerkannt.

03 Tokenisierung
Feldgenauer Ersatz sensibler Werte, stark in CRM, ERP, Gesundheits- und Finanzdaten. Detokenisierung nur innerhalb der EU-Domäne.

04 Verschlüsselung mit EU-Schlüsselhoheit
Customer Managed Keys sind Minimum, Bring Your Own Key besser, Hold Your Own Key am stärksten: Schlüssel liegen physisch außerhalb der Anbieter-Reichweite, etwa in einem EU-HSM.

05 Client-Side Encryption
Verschlüsselung vor dem Upload; der Anbieter sieht nie Klartext. Sehr stark, funktional aber auf Speicher- und Transportszenarien begrenzt.

06 Confidential Computing
Verarbeitung in Trusted Execution Environments: Daten bleiben auch **während der Berechnung** verschlüsselt, Remote Attestation belegt die Integrität der Umgebung. Schließt die Lücke zwischen „verschlüsselt speichern" und „im Klartext verarbeiten" und wird damit zur Schlüsseltechnologie für KI-Workloads mit sensiblen Daten.[22]

07 Zero-Retention-Konfiguration für KI
Vertraglich und technisch sicherstellen: keine Prompt-Speicherung, kein Training auf Ihren Daten, definierte Log-Fristen, EU-Verarbeitungsregion.

08 Private Deployments
Open-Weight-Modelle selbst betreiben (on-prem oder EU-VPC). Volle Kontrolle über Daten und Gewichte, dafür Betriebsverantwortung.

09 Gateway- statt Direktanbindung
Die wichtigste Architekturentscheidung, siehe unten.

10 Exit-Fähigkeit als Designkriterium
Offene Formate, dokumentierte Export-Pfade, vertragliche Wechselrechte. Der EU Data Act (voll anwendbar seit 12. September 2025) verpflichtet Anbieter, den Wechsel technisch zu ermöglichen.[26]

8.2 DIE GATEWAY-ARCHITEKTUR: MODELLE AUSTAUSCHBAR MACHEN

Wer Anwendungen direkt gegen die API eines einzelnen US-Anbieters baut, kettet seine Prozesse an dessen Rechtslage. Die resiliente Alternative schaltet eine eigene Kontrollschicht dazwischen:

```
ANWENDUNG → GATEWAY (AUTH · LOGGING · BUDGET)
              → POLICY-SCHICHT (DATENKLASSE · PII-FILTER · ROUTING)
              → MODELL-POOL (US-API | EU-API | LOKAL)
```

Der Effekt: Datenklassen entscheiden über das Routing (sensible Inhalte gehen an EU-gehostete oder lokale Modelle), jeder Aufruf ist auditierbar, und wenn eine Rechtsgrundlage fällt, wird der betroffene Endpunkt umkonfiguriert statt die Anwendung umgebaut. Ein Urteil wird so vom Architekturproblem zum Konfigurationsereignis.

DER 7-STUFEN-PLAN FÜR DIE NÄCHSTEN 12 MONATE

Kein Programm für den Krisenfall, sondern ein Vorgehen aus der Position der Stärke: erst Transparenz, dann Bewertung, dann Umbau. Jede Stufe erzeugt für sich genommen verwertbare Ergebnisse.

STUFE	MASSNAHME	ERGEBNIS	HORIZONT
01	**US-Exposure inventarisieren**	Transfer-Mapping aus dem Verfahrensverzeichnis: alle SaaS-, Cloud- und KI-Dienste mit US-Bezug, je Fluss die Rechtsgrundlage (DPF-Zertifizierung, SCC, Art. 49). Fernzugriffe und Sub-Dienstleister einschließen.	WOCHE 1–2
02	**Kritikalität klassifizieren**	Ampelmodell je Datenfluss (siehe unten). Priorisierung: Beschäftigten-, Gesundheits-, Finanz- und Kundendaten zuerst.	WOCHE 2–4
03	**Vendor Due Diligence**	Standardisierter Fragenkatalog an alle US-Anbieter (Seite 17). Antworten dokumentieren, Lücken terminieren.	WOCHE 4–8
04	**TIAs aktualisieren**	Neubewertung mit den Fakten seit dem 29. Juni 2026, dokumentierte Risikoentscheidung der Geschäftsführung. Besonders für KI-Workloads.	WOCHE 4–8
05	**SCC-Fallback vorbereiten**	Erst Bestand prüfen: Bei Hyperscalern ist der SCC-Fallback oft schon im AVV verankert (Kap. 7.1). Für die übrigen kritischen Anbieter Klauselwerke und Anhänge vorbereitet in der Schublade, nicht erst im Krisenmodus verhandelt.	MONAT 2–3
06	**Technische Controls umsetzen**	Reihenfolge nach Hebel: Schlüsselhoheit, Pseudonymisierung, Gateway-Schicht, Confidential Computing für sensible KI-Workloads.	MONAT 3–9
07	**KI-Governance & Exit verankern**	Verbindliche Policy, welche Datenklassen in welche KI-Systeme dürfen; Exit-Strategie je Kern-Workload; Integration in NIS2-Risikomanagement und Managementbericht.	MONAT 3–12

9.1 DAS AMPELMODELL FÜR STUFE 02

ROT · STOPP-PRÜFUNG

Personenbezogen, sensibel oder geschäftskritisch: Gesundheits-, HR-, Finanzdaten, Geschäftsgeheimnisse in Prompts. Nur mit wirksamen technischen Maßnahmen oder EU-Alternative.

GELB · BEDINGT

Personenbezogen, aber begrenzt: geschäftliche Kontaktdaten, pseudonymisierbare Vorgänge. Zulässig mit dokumentiertem TIA und Zusatzmaßnahmen.

GRÜN · UNKRITISCH

Kein Personenbezug: Maschinendaten, öffentliche Inhalte, synthetische Testdaten. Frei nutzbar, Klassifikation trotzdem dokumentieren.

VENDOR-FRAGENKATALOG UND KI-DATENREGELN

9.2 ZWÖLF FRAGEN AN JEDEN US-ANBIETER

Schriftlich stellen, Antworten archivieren. Ausweichende Antworten sind selbst ein Prüfungsergebnis.

01 Sind Sie aktuell DPF-zertifiziert? Was ist Ihr dokumentierter Plan für den Fall des Wegfalls?

02 Liegen unterschriftsreife SCC (Modul-zugeordnet) mit allen Anhängen vor?

03 In welcher Region werden unsere Daten verarbeitet, nicht nur gespeichert?

04 Welche Konzerngesellschaften und Sub-Dienstleister haben technischen Zugriff, aus welchen Jurisdiktionen?

05 Bieten Sie CMK, BYOK oder HYOK an? Wo liegt das Schlüsselmaterial physisch?

06 Unterstützen Sie Client-Side Encryption oder Confidential-Computing-Optionen?

07 Für KI-Dienste: Zero Retention verfügbar? Trainingsausschluss vertraglich zugesichert?

08 Wie viele Behördenanfragen auf EU-Kundendaten hatten Sie in 24 Monaten? (Transparenzbericht)

09 Verpflichten Sie sich, Herausgabeverlangen anzufechten und uns soweit zulässig zu informieren?

10 Welche Exportformate und -wege existieren für einen vollständigen Datenabzug?

11 Welche Wechselunterstützung leisten Sie nach EU Data Act, zu welchen Kosten?

12 Existiert eine EU-Betreibergesellschaft mit eigener Infrastruktur, oder nur eine Vertriebsentität?

9.3 KI-GOVERNANCE: DIE VIER-ZEILEN-POLICY ALS KERN

Die wirksamste KI-Datenregel ist die, die jeder Beschäftigte auswendig kann. Der Kern lässt sich in vier Zuordnungen fassen, alles Weitere ist Ausgestaltung:

DATENKLASSE	ZULÄSSIGE SYSTEME
Grün (kein Personenbezug)	Alle freigegebenen KI-Dienste.
Gelb (begrenzt personenbezogen)	Nur Dienste mit dokumentiertem TIA, EU-Region und Zero Retention; Pseudonymisierung vor Eingabe.
Rot (sensibel/kritisch)	Nur EU-gehostete oder lokal betriebene Modelle, ideal hinter dem eigenen Gateway; Klartext verlässt die kontrollierte Domäne nicht.
Schwarz (Verschlusssachen, Berufsgeheimnisse)	Keine Cloud-KI. Ausschließlich dedizierte, geprüfte Umgebungen.

PRAXISWARNUNG AUS DEM FEBRUAR 2025

Als die US-Regierung im Februar 2025 Sanktionen gegen den Chefankläger des Internationalen Strafgerichtshofs verhängte, verlor dieser in der Folge den Zugriff auf sein Microsoft-E-Mail-Konto und wechselte zu einem Schweizer Anbieter. Microsoft widersprach der Darstellung einer „Sperrung" ausdrücklich: Man habe zu keinem Zeitpunkt Dienste für den Gerichtshof eingestellt, die Trennung des Kontos sei in Abstimmung mit dem IStGH erfolgt.[23] Unabhängig von der Bewertung im Einzelfall bleibt die Lehre: Verfügbarkeit hat eine Compliance-Dimension. Wer geschäftskritische Prozesse betreibt, plant den Zugriffsverlust ein, nicht nur den Datenabfluss.

SOUVERÄNE OPTIONEN: DER MARKT IM ÜBERBLICK

Der Markt hat sich 2025/2026 spürbar bewegt: Milliardeninvestitionen, neue Angebote, und mit dem Cloud Sovereignty Framework der EU-Kommission (Oktober 2025) erstmals ein offizieller Bewertungsrahmen mit Souveränitätsstufen von SEAL-0 bis SEAL-4 für die Beschaffung.[24] Entscheidend ist, drei Kategorien sauber zu unterscheiden, denn „souverän" steht auf sehr unterschiedlichen Etiketten.

KATEGORIE	BEISPIELE	EINORDNUNG
EU-native Anbieter (EU-Eigentum, EU-Recht, EU-Betrieb)	STACKIT (Schwarz Digits) · Open Telekom Cloud · IONOS · plusserver · Hetzner · OVHcloud · Nextcloud/Kollaboration	Klarste Rechtslage, kein CLOUD-Act-Durchgriff. Funktionsumfang je Workload prüfen; Reifegrad steigt schnell: Schwarz Digits investiert 11 Mrd. Euro in ein KI-Rechenzentrum in Lübbenau, erster Bauabschnitt bis Ende 2027.[28]
Treuhand- & Schlüsselmodelle (US-Technologie, EU-Kontrolle)	T-Systems Sovereign Cloud (Google-Basis, Schlüsselverwaltung bei T-Systems) · Delos Cloud (SAP-Tochter, Microsoft-Basis, öffentl. Sektor: Pilotbetrieb, Markteintritt 2026)	Kompromiss aus Funktionsumfang und Kontrolle: Betrieb bzw. Schlüssel bei einem EU-Treuhänder, der Cloud-Betreiber hat keinen Zugriff auf das Schlüsselmaterial. Governance-Details entscheiden über die tatsächliche Schutzwirkung.[25][35]
Hyperscaler-„Sovereign"-Angebote (US-Eigentum, EU-Verpackung)	AWS European Sovereign Cloud (erste Region Brandenburg, seit 15.01.2026) · Microsoft EU Data Boundary (fertiggestellt 02/2025) · Google Sovereign Portfolio	Reale Fortschritte bei Residenz, Personal und Metadaten. Der Jurisdiktionskonflikt bleibt jedoch bestehen, solange die Muttergesellschaft US-Recht unterliegt. Kritiker sprechen von „Sovereignty Washing".[21][29][30]

10.1 MACHBARKEIT: DER NORDEN HAT ES VORGEMACHT

Dass Migration kein theoretisches Konzept ist, zeigt Schleswig-Holstein: Nach Angaben der Staatskanzlei arbeiteten Ende 2025 fast 80 Prozent der rund 30.000 Arbeitsplätze der Landesverwaltung (außerhalb der Steuerverwaltung) mit LibreOffice statt Microsoft Office, die Migration von rund 44.000 E-Mail-Postfächern auf Open-Xchange war bereits abgeschlossen. Das Land beziffert die eingesparten Lizenzkosten auf mehr als 15 Mio. Euro, denen einmalige Umstellungskosten von rund 9 Mio. Euro gegenüberstehen.[27] Für den Mittelstand gilt dieselbe Mechanik in klein: Sechs bis achtzehn Monate je Workload sind eine realistische Planungsgröße, deutlich günstiger als jede Notfallmigration.

Wie groß die Lücke zwischen Risikobewusstsein und Vorbereitung ist, zeigt eine Lünendonk-Erhebung vom März 2026 unter IT-Verantwortlichen in der DACH-Region: 83 Prozent halten ein Kill-Switch-Szenario, also das politisch veranlasste Abschalten von Cloud-Diensten, grundsätzlich für realistisch. Aber nur 57 Prozent haben eine dokumentierte Exit-Strategie; 43 Prozent haben keine.[18]

10.2 DIE RICHTIGE REIHENFOLGE

Nicht alles muss migrieren. Ein gestuftes Modell trägt weiter als Maximalforderungen: Rote Workloads (Kap. 09) auf EU-native oder Treuhandmodelle, gelbe Workloads mit Schlüsselhoheit und Zusatzmaßnahmen dort belassen, wo sie sind, grüne Workloads nach Wirtschaftlichkeit. Souveränität entsteht durch Handlungsfähigkeit, nicht durch Abschottung.

DIE STRATEGISCHE KONSEQUENZ: ARCHITEKTUR SCHLÄGT ABKOMMEN

Safe Harbor hielt fünfzehn Jahre. Privacy Shield vier. Das DPF steht nach drei Jahren ohne tragende Begründung da. Wer daraus nur ableitet, das nächste Abkommen abzuwarten, hat das Muster nicht verstanden.

Der eigentliche Befund dieses Papiers ist unbequem und befreiend zugleich: Die Stabilität Ihrer Datenverarbeitung hängt nicht an Brüsseler Beschlüssen, Washingtoner Urteilen oder den Zusagen einzelner Anbieter. Sie hängt an Entscheidungen, die Sie selbst treffen: Welche Daten verlassen Ihre Kontrolldomäne im Klartext? Wer hält die Schlüssel? Wie schnell können Sie einen Anbieter ersetzen?

Diese Fragen beantwortet kein Vertrag. Sie beantwortet Architektur. Und Architektur ist, anders als transatlantische Diplomatie, vollständig in Ihrer Hand.

> **Datensouveränität heißt nicht, auf US-Technologie zu verzichten. Datensouveränität heißt, dass ein Gerichtsurteil in Washington Ihr Unternehmen nicht stoppen kann.**

11.1 DREI GRUNDSÄTZE FÜR DIE KOMMENDEN 24 MONATE

Rechtsgrundlagen sind Wetter, Architektur ist Klima. Bauen Sie Systeme, die einen Wechsel der Transfergrundlage als Konfigurationsereignis behandeln, nicht als Krisenprojekt. Gateway-Schichten, Schlüsselhoheit und Exit-Pfade sind die Instrumente dafür.

Klassifikation vor Technologie. Die meisten Unternehmen wissen präziser, welche Laptops sie besitzen, als welche personenbezogenen Daten ihre KI-Werkzeuge verlassen. Transparenz über Datenflüsse ist die Voraussetzung jeder weiteren Entscheidung, und sie ist in Wochen herstellbar, nicht in Jahren.

Souveränität ist ein Portfolio, kein Bekenntnis. Rote Workloads unter EU-Kontrolle, gelbe mit technischen Garantien, grüne nach Wirtschaftlichkeit. Wer so sortiert, nutzt die Innovationsgeschwindigkeit des Weltmarkts, ohne sein Schicksal an eine fremde Jurisdiktion zu ketten.

11.2 DAS ZEITFENSTER

Es gibt einen seltenen Moment in regulatorischen Zyklen: nach dem Warnschuss, vor dem Einschlag. In diesem Moment befinden wir uns. Die Verfahren sind anhängig, die Argumente liegen auf dem Tisch, die Zeithorizonte sind bekannt. Alles, was in Kapitel 09 beschrieben ist, lässt sich heute in Ruhe, zu Normalkonditionen und mit Auswahl unter Anbietern umsetzen. Dieselben Maßnahmen nach einem EuGH-Urteil kosten ein Mehrfaches und werden unter Zeitdruck schlechter.

Die Unternehmen, die 2020 auf Schrems II vorbereitet waren, hatten keinen besseren Anwalt. Sie hatten früher angefangen.

DER US-EXPOSURE-SCHNELLCHECK

Zehn Fragen, ehrlich beantwortet. Jedes „Nein" ist ein Punkt. Zählen Sie mit.

NR	AUSSAGE	JA	NEIN
01	Wir haben ein aktuelles Inventar aller US-Dienste, die personenbezogene Daten verarbeiten.	☐	☐
02	Für jeden dieser Datenflüsse ist die Rechtsgrundlage dokumentiert (DPF, SCC, Art. 49).	☐	☐
03	Unsere Transfer Impact Assessments wurden nach dem 29. Juni 2026 überprüft.	☐	☐
04	Wir wissen, welche Prompts, Logs und KI-Kontexte unser Haus in Richtung USA verlassen.	☐	☐
05	Es existiert eine verbindliche Regel, welche Datenklassen in welche KI-Systeme dürfen.	☐	☐
06	Für unsere sensibelsten Daten in US-Diensten halten wir die Schlüssel selbst (BYOK/HYOK).	☐	☐
07	Unterschriftsreife SCC liegen für unsere kritischen US-Anbieter bereit.	☐	☐
08	KI-Anwendungen laufen über eine eigene Gateway-Schicht, nicht direkt gegen Anbieter-APIs.	☐	☐
09	Für jeden kritischen Workload existiert eine dokumentierte, getestete Exit-Option.	☐	☐
10	Die Geschäftsführung hat die Restrisiko-Entscheidung zu US-Transfers schriftlich getroffen.	☐	☐

0–2 NEIN · SOLIDE

Sie gehören zur vorbereiteten Minderheit. Halten Sie den Stand, beobachten Sie die Verfahren, testen Sie Ihre Exit-Pfade einmal jährlich.

3–5 NEIN · LÜCKENHAFT

Typisches Mittelfeld: Grundlagen vorhanden, KI-Flüsse und Schlüsselhoheit offen. Stufen 01 bis 04 des Plans schließen die kritischsten Lücken in acht Wochen.

6–10 NEIN · EXPONIERT

Ein EuGH-Urteil träfe Sie unvorbereitet, eine Behördenanfrage ebenso. Beginnen Sie diese Woche mit Stufe 01. Nicht aus Angst, sondern weil jede Woche Vorsprung später Verhandlungsmacht ist.

QUELLEN

Alle Quellen zuletzt geprüft am 3. Juli 2026. Primärquellen (Gerichte, Gesetzgeber, offizielle Stellen, Unternehmensmitteilungen) sind den Analysen und Presseberichten vorangestellt.

PRIMÄRQUELLEN

[1] US Supreme Court: Trump v. Slaughter, No. 25-332, Urteil vom 29.06.2026 (Slip Opinion). supremecourt.gov/opinions/25pdf/25-332_qn12.pdf

[2] Europäische Kommission: Durchführungsbeschluss (EU) 2023/1795 vom 10.07.2023 (EU-US Data Privacy Framework). EUR-Lex

[3] noyb: „US Supreme Court just blew up EU-US Data Transfers" sowie formelles Schreiben an die EU-Kommission, beide 29.06.2026. noyb.eu/en/us-supreme-court-just-blew-eu-us-data-transfers

[5] Gericht der Europäischen Union: Urteil vom 03.09.2025, Rs. T-553/23 (Latombe/Kommission); Rechtsmittel anhängig als C-703/25 P (eingelegt 31.10.2025). curia.europa.eu

[6] EuGH: Urteile vom 06.10.2015, C-362/14 (Schrems I) und vom 16.07.2020, C-311/18 (Schrems II). curia.europa.eu

[7] Europäischer Datenschutzausschuss: Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools, Version 2.0 vom 18.06.2021 (Use Cases 1, 6, 7); ergänzend Empfehlungen 02/2020 (European Essential Guarantees). edpb.europa.eu

[8] Microsoft: „Protecting privacy as a fundamental right while supporting transatlantic data flows", 28.06.2026. blogs.microsoft.com/on-the-issues

[15] Congress.gov: H.R. 4943, CLOUD Act (P.L. 115-141, in Kraft seit 23.03.2018; Herausgabepflicht nach 18 U.S.C. § 2713 unabhängig vom Speicherort). congress.gov

[20] BfDI: Themenseite Internationale Datenübermittlung; DSK-Anwendungshinweise zum EU-US DPF. bfdi.bund.de

[24] Europäische Kommission: Cloud Sovereignty Framework (Bewertungsrahmen für die Beschaffung, Souveränitätsstufen SEAL-0 bis SEAL-4), 10.10.2025. commission.europa.eu

[25] T-Systems: „Sovereign Cloud powered by Google Cloud" (External Key Management durch T-Systems, kein Schlüsselzugriff des Cloud-Betreibers). t-systems.com

[26] EUR-Lex: Verordnung (EU) 2023/2854 (Data Act) vom 13.12.2023, anwendbar seit 12.09.2025; Wechselpflichten in Kapitel VI (Art. 23 ff.). eur-lex.europa.eu/eli/reg/2023/2854/oj

[27] Staatskanzlei Schleswig-Holstein: „LibreOffice ersetzt Microsoft: Schon fast 80 Prozent der Arbeitsplätze umgestellt", Pressemitteilung vom 04.12.2025. schleswig-holstein.de

[28] Schwarz Digits: „Spatenstich in Lübbenau: Schwarz Digits investiert 11 Milliarden Euro in Europas digitale Souveränität", Pressemitteilung vom 17.11.2025. schwarz-digits.de

[29] Amazon: „AWS Launches AWS European Sovereign Cloud" (erste Region Brandenburg), Pressemitteilung vom 15.01.2026. press.aboutamazon.com

[30] Microsoft: „Microsoft completes landmark EU Data Boundary", 26.02.2025. blogs.microsoft.com/on-the-issues

[31] Europäisches Parlament: Entschließung vom 11.05.2023 zur Angemessenheit des Schutzes durch das EU-US Data Privacy Framework (2023/2501(RSP)), u. a. Ziff. 9 zum DPRC. europarl.europa.eu

[32] EDPB: Opinion 5/2023 zum Entwurf des Angemessenheitsbeschlusses, 28.02.2023. edpb.europa.eu

[33] Lawfare: „Trump's Sacking of PCLOB Members Threatens Data Privacy", 31.01.2025. lawfaremedia.org

[34] EuGH: Jahresstatistik der Rechtsprechungstätigkeit 2024 (durchschnittliche Dauer der Rechtsmittelverfahren: 18,4 Monate). curia.europa.eu

[35] Delos Cloud: Unternehmensmeldungen 01–06/2026 (Betriebsbereitschaft der Infrastruktur, Pilotkunden, Markteintritt mit Launch-Partnern). deloscloud.de

STUDIEN, ANALYSEN UND BERICHTERSTATTUNG

STUDIEN, ANALYSEN UND BERICHTERSTATTUNG

[4] heise online: „Kartenhaus: Wie ein US-Urteil den transatlantischen Datenfluss sprengen könnte", 30.06.2026 (dt./engl. Fassung). heise.de

[9] DSN Group, datenschutz notizen: „US Supreme Court erklärt Unabhängigkeit der FTC für verfassungswidrig", 01.07.2026. dsn-group.de

[10] KPMG Klardenker: „Steht das EU-US Data Privacy Framework vor dem Aus?", Januar 2026. klardenker.kpmg.de

[11] Tagesspiegel Background: „US-Urteil bringt EU-US-Datentransfers unter Druck", 30.06.2026. background.tagesspiegel.de

[12] Mrak: „Trump v. Slaughter: Dem EU-US-Datentransfer fehlt jetzt die Rechtsgrundlage" und „Microsoft verteidigt das Data Privacy Framework", 06/07-2026. mrak.at

[13] Börse Express: „Datentransfer USA: Supreme-Court-Urteil stellt EU-Abkommen infrage", 01.07.2026. boerse-express.com

[14] Provectus: „US-Urteil zur FTC: Was Microsoft-Kunden jetzt prüfen sollten", 01.07.2026. provectus.de

[16] Heuking: „EuG confirms effectiveness of EU-US Data Privacy Framework", 03.09.2025. heuking.de

[17] heise online: „Data transfer to US: lawsuit against EU data protection framework goes to ECJ", 30.10.2025. heise.de

[18] Lünendonk & Hossenfelder: Studie „Digitale Souveränität. Vom Risiko zur Resilienz", März 2026 (Befragung von 155 IT-Verantwortlichen in der DACH-Region, 12/2025–01/2026). luenendonk.de

[19] Dr. Web: „Ist der EU-US-Datentransfer nach DPF noch sicher?", 01.07.2026. drweb.de

[21] digitalbusiness magazin: „Digitale Souveränität: die Illusion der Unabhängigkeit", 05/2026. digitalbusiness-magazin.de

[22] Börse Express: „Datenschutz-Schock: US-Urteil gefährdet EU-Datenaustausch" (u. a. zur Rolle von Confidential Computing), 02.07.2026. boerse-express.com

[23] AP News: „Trump's sanctions on ICC prosecutor have halted tribunal's work", 15.05.2025 (apnews.com); Microsoft-Gegendarstellung: Politico, „Microsoft did not cut services to ICC", 06/2025 (politico.eu)

punkt.exe

Punktexe ist die Beratung für sichere KI-Transformation im Mittelstand. Wir bringen Unternehmen kontrolliert in die KI-Nutzung: mit klarer Standortbestimmung, belastbarer Governance und Architekturen, die Souveränität nicht versprechen, sondern herstellen. Regulierung wie DSGVO, EU AI Act und NIS2 übersetzen wir in Architektur- und Prozessentscheidungen, die im Betrieb funktionieren. Kein Papier für den Ordner, sondern Systeme, die Prüfungen und regulatorische Schocks überstehen.

KI-STANDORTBESTIMMUNG

Der strukturierte Einstieg: KI-Betriebsreife-Check über fünf Dimensionen (Datenzugriff, Modell-Risiko, Prozessreife, Governance, Sicherheit) mit Ampel-Bewertung, Risiko- und Governance-Analyse und einer 30/60/90-Tage-Roadmap. Das US-Exposure-Mapping der Stufen 01 bis 04 aus Kapitel 09 ist hier Teil der Risikoanalyse.

→ **punktexe.de/ki-standortbestimmung/**

SICHERES KI-TRANSFORMATIONSPROGRAMM

Die modulare Umsetzung: KI-Härtung & Resilienz (Guardrails, PII-Maskierung, Auditierbarkeit, Failover), Infrastruktur-Design mit Gateway-Architektur und Schlüsselhoheit, Enablement für Ihre Teams. Genau die Maßnahmen aus Kapitel 08, gebaut für Ihren Betrieb.

→ **punktexe.de/ki-transformationsprogramm/**

Sprechen wir über Ihre Exponierung, bevor es ein Gericht tut.

→ PUNKTEXE.DE/KONTAKT/ · WWW.PUNKTEXE.DE