punkt.exe
PUNKTEXE RESEARCH

WHITEPAPER · JULY 2026
AS OF JULY 3, 2026 · V1.1 (EN)

EU-US DATA PRIVACY FRAMEWORK · TRUMP V. SLAUGHTER · GDPR CHAPTER V

TRANSFER ON BORROWED TIME.

A ruling in Washington calls the legal basis of transatlantic data flows into question. What this means for German companies, which clocks are now ticking, and how you build architectures that survive regulatory shocks.

JUNE 29, 2026 · SCOTUS 6:3

TRUMP V. SLAUGHTER, NO. 25-332: FTC INDEPENDENCE RULED UNCONSTITUTIONAL

259×

REFERENCES TO THE FTC IN THE EU ADEQUACY DECISION (EU) 2023/1795

3rd attempt

AFTER SAFE HARBOR (†2015) AND PRIVACY SHIELD (†2020), THE DPF IS NOW ON SHAKY GROUND

FOR DECISION-MAKERS IN IT, LEGAL & EXECUTIVE MANAGEMENT · WWW.PUNKTEXE.DE

WHAT TO EXPECT ON THE FOLLOWING PAGES

ACT I · THE RULING

ACT II · THE RISK PICTURE

ACT III · THE RESPONSE

TOOLKIT & APPENDIX

SHORT ON TIME? Executive management: p. 03, 10, 20 · IT & security: ch. 08–09 · Legal & privacy: ch. 01–07

A NOTE ON CONTEXT

This whitepaper was finalized on July 3, 2026, four days after the US Supreme Court ruling. The situation continues to evolve. All legal statements are provided for information purposes and do not replace legal advice in individual cases. Statements marked as a “Punktexe assessment” are reasoned evaluations, not predictions.

THE ESSENTIALS ON ONE PAGE

On June 29, 2026, the US Supreme Court declared the statutory independence of the Federal Trade Commission unconstitutional. That very independence was a load-bearing assumption of the EU-US Data Privacy Framework, the most important legal basis for data transfers to the United States.

6:3

MAJORITY ON THE SUPREME COURT. IT OVERTURNS A PRECEDENT FROM 1935 (HUMPHREY'S EXECUTOR)

259×

TIMES THE EU ADEQUACY DECISION RELIES ON THE FTC AS INDEPENDENT OVERSIGHT

2–3 years

IS THE TYPICAL DURATION OF CJEU PROCEEDINGS. THE LATOMBE APPEAL HAS BEEN PENDING SINCE OCT. 2025

01 NOTHING IS PROHIBITED TODAY. BUT THE RATIONALE IS GONE.

The adequacy decision formally remains in force until the European Commission repeals it or the CJEU declares it invalid. There are no automatic fines and no obligation to pull the plug tomorrow. But the decision's load-bearing argument, an independent US supervisory authority, has not existed since June 29.

02 SCC USERS ARE ON THE HOOK NOW, NOT JUST “IF IT FALLS.”

If you base transfers on standard contractual clauses or Binding Corporate Rules, you must update your transfer impact assessment now. These assessments typically cite the FTC, the PCLOB, and the Data Protection Review Court as independent oversight bodies. Under the logic of the ruling, all three assumptions are void.

03 AI SYSTEMS MULTIPLY YOUR EXPOSURE.

Prompts, RAG contexts, agent logs, and meeting recordings are personal data flows in real time. If you use Copilot, ChatGPT, or US-hosted models, you have more transfers than your records of processing activities suggest.

04 ALMOST NOTHING WORKS EXCEPT TECHNICAL MEASURES.

The European Data Protection Board considers purely contractual and organizational supplementary measures insufficient. What holds: encryption with key control in the EU, pseudonymization before transfer, confidential computing, gateway architectures with interchangeable models.

05 THE PLANNING ASSUMPTION: A 12 TO 24 MONTH PREPARATION WINDOW.

Nothing falls in the short term. In the medium term, a “Schrems III” is realistic. Those who inventory, classify, and build key sovereignty now act from strength. Those who wait will act later under time pressure, at crisis terms.

> **The real question is not whether you use US technology. The question is whether a court ruling in Washington can stop your business.**

A RULING IN WASHINGTON. CONSEQUENCES IN EUROPE.

Trump v. Slaughter reads like a domestic constitutional dispute over presidential power. In fact, the decision strikes the load-bearing pillar on which a substantial share of European cloud and AI usage legally rests.

WHAT WAS DECIDED ON JUNE 29

By a 6:3 vote, the US Supreme Court held in Trump v. Slaughter (No. 25-332) that the statutory removal protection for commissioners of the Federal Trade Commission is unconstitutional.[1]

The trigger was the removal of the Democratic FTC commissioners Rebecca Slaughter and Alvaro Bedoya in spring 2025, at the start of President Trump's second term. Both were dismissed without the statutorily required grounds such as misconduct or neglect of duty. The lower courts had still classified the dismissals as unlawful. The Supreme Court saw it differently and sided with the administration.[4][11]

1.1 A PRECEDENT FROM 1935 FALLS

The decision overrules Humphrey's Executor v. United States from 1935. For roughly nine decades, the rule was: Congress may equip members of independent regulatory agencies with removal protection, and dismissal is possible only “for cause.” This construction shielded the FTC and about two dozen other agencies from direct political interference.[4][12] Only for the Federal Reserve did the Court explicitly formulate an exception.[1]

1.2 THE REASONING: UNITARY EXECUTIVE THEORY

The conservative majority follows the so-called unitary executive theory. Under this reading of the Constitution, the president must hold unrestricted control over all executive agencies. Statutory provisions that shield individual agencies from direct presidential control are therefore unconstitutional.[4]

WHY THIS IS NOT A PURELY US ISSUE

The ruling's logic is not limited to the FTC. It structurally reaches every US executive body whose independence was previously secured by statute or executive order. It thereby hits exactly the building blocks with which the US demonstrated an “equivalent level of data protection” to the EU: independent oversight and independent redress.

1.3 THE IMMEDIATE REACTION

The very night after the ruling, the privacy organization noyb, led by Max Schrems, formally called on the European Commission in a letter to repeal the adequacy decision for the US in an orderly procedure. The reasoning: after the ruling, there are simply no independent supervisory authorities left in the US for the EU to rely on. An action for annulment was announced for the coming weeks.[3]

First political reactions came from the European Parliament: the data protection agreement had collapsed, the Commission needed to act, and the answer lay in European digital sovereignty.[13] As of this paper's editorial deadline, the Commission itself had not taken a formal position; a spokesperson merely announced a review of whether the ruling affects the validity of the DPF. Observers expect it to take its time: a quick withdrawal from the agreement is considered politically and economically almost inconceivable.[14]

THE TRANSATLANTIC CHAIN: WHY THE FTC CARRIES THE DPF

To understand why a US constitutional ruling hits European data protection law, you need to know the chain from which transatlantic data flows hang. It has five links. The ruling severs two of them.

NO	LINK	FUNCTION
1	**Art. 44 et seq. GDPR**	Personal data may only go to third countries if the level of protection there is “essentially equivalent.” A principle since 1995.
2	**Art. 45 GDPR: adequacy decision**	The European Commission can determine by decision that a third country offers adequate protection. Data then flows without further instruments.
3	**Implementing Decision (EU) 2023/1795**	The current decision for the US, in force since July 10, 2023: the EU-US Data Privacy Framework (DPF).[2]
4	**Independent oversight: the FTC**	EU primary law (Art. 16(2) TFEU, Art. 8(3) of the Charter of Fundamental Rights (CFR)) strictly requires independent data protection oversight. In the US, the FTC fills that role. By noyb's count, the decision references it 259 times.[3][4]
5	**Redress: EO 14086, DPRC, PCLOB**	Executive Order 14086 (2022) limits intelligence access, creates the Data Protection Review Court (DPRC), and relies on oversight by the Privacy and Civil Liberties Oversight Board (PCLOB).[2][12]

2.1 LINK 4 HAS SNAPPED

After the ruling, the FTC is subject to the president's direct authority. The independence the Commission invokes 259 times in its decision is thus gone as a load-bearing assumption. Other bodies named in the decision, such as the Department of Transportation, have no comparable enforcement function and, as executive agencies, are subject to the same ruling logic.[12]

2.2 LINK 5 WAS ALREADY DAMAGED

The DPRC is not a court within the meaning of Art. 47 of the EU Charter of Fundamental Rights but a body within the US Department of Justice. Its independence rests solely on a presidential order that can be revoked at any time. This criticism is not new: as early as 2023, the European Parliament found that the DPRC does not meet the independence and impartiality requirements of Art. 47 CFR.[31][32] The PCLOB has lacked a quorum since the removal of three of its members in January 2025 and can perform its oversight function only to a limited extent.[9][12][33]

> **EU primary law demands independent oversight. The US Constitution, as now read, prohibits it. This contradiction cannot be resolved by elections or by the promises of individual corporations.**

The conflict could only be resolved by a unanimous amendment of the EU treaties or a realignment of US constitutional law. Neither is in sight for the foreseeable future.[12]

A PATTERN FORETOLD: STRUCK DOWN TWICE, SHAKY ONCE

The current situation is no accident. It is the third rerun of the same conflict: EU fundamental rights protection meets US surveillance law. The CJEU has ruled twice already. Both times against the agreement.

● 2000–2015

SAFE HARBOR

Struck down on October 6, 2015 by Schrems I (CJEU, C-362/14). Core problem: US mass surveillance, lack of redress.

● 2016–2020

PRIVACY SHIELD

Struck down on July 16, 2020 by Schrems II (CJEU, C-311/18). Core problem: FISA 702, EO 12333, no effective remedy.

● 2023–?

DATA PRIVACY FRAMEWORK

In force since July 10, 2023. EGC action dismissed (9/2025), appeal pending before the CJEU, without a load-bearing rationale since June 29, 2026.

○ 2027+

"SCHREMS III"?

The Latombe appeal and the announced noyb action make a third CJEU ruling a realistic scenario.

3.1 THE STRUCTURAL PROBLEM REMAINS THE SAME

Both predecessors failed at identical hurdles: Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333 allow US intelligence services broad access to the data of non-US persons, who have no equivalent legal remedy. The CLOUD Act, added in 2018, obliges US providers to hand over data under their control, regardless of where it is stored.[6] [15]

The DPF was meant to defuse this criticism through Executive Order 14086: a proportionality principle for data collection, a complaint path via the DPRC, oversight by the PCLOB. The design flaw: everything essential rests on executive commitments rather than an act of Congress. Exactly this fragility has been materializing piece by piece since 2025: the PCLOB paralyzed, DPRC independence called into question, FTC independence struck down.[7][12]

3.2 WHAT IS DIFFERENT THIS TIME

Schrems I and II were about surveillance powers, that is, about what US law **permits**. Trump v. Slaughter is about what US constitutional law **prohibits**: precisely the kind of independent oversight that EU law strictly requires. As long as this constitutional case law stands, the conflict is, for the first time, not politically negotiable. No fourth agreement can make an agency independent when the highest US court has declared its independence unconstitutional.

FORMALLY VALID. MATERIALLY HOLLOWED OUT.

The Data Privacy Framework remains in force, and that is exactly what makes the situation treacherous: there is no alarm, no deadline, no warning letter in the mail. Just a legal basis whose rationale no longer exists, and three procedural paths on which it can fall.

THREE PATHS ON WHICH THE DPF CAN FALL

The adequacy decision will not disappear on its own. It remains effective until the Commission revokes it or the CJEU declares it invalid. As long as it stands, the supervisory authorities are bound by it too and may not impose fines for DPF-based transfers.[16] What matters, therefore, is which proceedings are now underway and how fast they move.

4.1 PATH 1: THE COMMISSION REVOKES IT ITSELF

noyb has formally called on the Commission to withdraw in an orderly manner.[3] Politically, this path is considered unlikely: a revocation would throw transatlantic data flows back onto derogations and standard contractual clauses overnight, in the middle of an already strained trade relationship. It is more realistic that the Commission will assess the ruling as part of its ongoing review obligation and play for time.[14]

4.2 PATH 2: THE LATOMBE APPEAL (ALREADY UNDERWAY)

The French MP Philippe Latombe had challenged the decision before the General Court of the EU. The EGC dismissed the action on September 3, 2025 (T-553/23), but expressly examined only the factual and legal situation at the time of the decision in July 2023. That departs from the CJEU's established standard, under which the time of the judicial review counts.[5][12] The appeal has been pending before the CJEU since October 31, 2025 under case number C-703/25 P. It can attack exactly this point, and Trump v. Slaughter hands the Court fresh material that is hard to ignore. Appeal proceedings most recently took 18.4 months on average (CJEU annual statistics 2024); a decision is therefore conceivable from 2027 onward.[12][17][34]

NOTEWORTHY: MICROSOFT JOINS THE PROCEEDINGS

On June 28, 2026, one day before the Supreme Court ruling, Microsoft announced that the Court had admitted the company as an intervener on the Commission's side in the Latombe proceedings.[8] The interest is legitimate and openly stated: the legal basis of a substantial part of its own business model is at stake. Legally, however, the intervention does not solve the core problem. Whether US law offers “essentially equivalent” protection is decided by the US legal order, not by the conduct of individual providers.[12]

4.3 PATH 3: THE ANNOUNCED NOYB ACTION (“SCHREMS III”)

noyb intends to file its own action for annulment against the decision in the coming weeks; it formally begins before the General Court (EGC). Experience shows such proceedings take two to three years across the instances.[3][11] The organization has already brought down two agreements before the CJEU, Safe Harbor and Privacy Shield. This time its central argument is simpler than ever: EU law requires independent oversight, and by the finding of the highest US court, that no longer exists in the United States.

> **Both judicial paths end before the same court that has already ruled against such an agreement twice. The third path hinges on the Commission's political will.**

SCENARIOS AND TIME HORIZONS: THE PUNKTEXE ASSESSMENT

Nobody can predict a court ruling, including us. What can be assessed responsibly: the strength of the arguments, the duration of the proceedings, and the consequences of each scenario. That is exactly what your planning should build on.

SCENARIO	DESCRIPTION	TIME HORIZON	ASSESSMENT
A · Grinding continuity	The Commission waits, proceedings drag on, the DPF formally remains in force. Legal uncertainty and due diligence obligations rise steadily.	2026–2028	Most likely scenario in the short term
B · "Schrems III"	The CJEU strikes down the decision (possible via the Latombe appeal from 2027, the noyb action more likely 2028/29). A transition period is uncertain; Schrems II had none.	2027–2029	Realistic; the probability has risen markedly
C · Orderly withdrawal	The Commission revokes the decision itself and negotiates transition rules. Legally clean, politically costly.	open	Unlikely without external pressure
D · Political escalation	Data transfers become a bargaining chip in the trade conflict; abrupt tightening on either side.	any time	Residual risk; cannot be planned for, but can be hedged

5.1 THE PLANNING ASSUMPTION

For corporate planning, this yields a clear working basis: **treat the DPF as a valid but finite legal basis.** As a formal transfer instrument, it lives. As a planning basis for architecture decisions with multi-year lifespans, it is unsuitable. The preparation window in which you can act on your own terms is, in our assessment, 12 to 24 months.

5.2 WHY WAITING GETS EXPENSIVE

With Schrems II, the Privacy Shield fell on the day the judgment was announced, with no transition period. Companies had to switch to SCCs within weeks and improvise supplementary measures. Those who were prepared signed amendments. Those who were not negotiated under time pressure with vendors that were processing thousands of identical requests at once. Migration projects born of necessity typically cost a multiple of planned ones, with six to eighteen months a realistic switching time per workload.

5.3 THE CASE AGAINST ALARM

The counterposition deserves to be taken seriously, because it has three valid arguments: the EGC dismissed the action against the DPF at first instance in 2025. The Commission can make adjustments, for instance by extracting improvements from the US side. And no supervisory authority has an interest in putting its own economy in the wrong overnight; some law firms accordingly advise calm rather than rushed action.

Except: all three arguments concern the pace, not the direction. They extend the preparation window; they do not close it. And none of them repairs the core issue that the decision's load-bearing assumption is gone. That is exactly why this paper's planning assumption is 12 to 24 months, and not zero.

THE PUNKTEXE ASSESSMENT IN ONE SENTENCE

Nothing falls in the short term, another failure before the CJEU is the realistic base risk in the medium term, and the only variable you control is your own level of preparation.

EXPOSURE: WHO IS AFFECTED AND WHY AI MAKES EVERYTHING WORSE

Practically every company that processes personal data through US services is affected. That means: email and collaboration (Microsoft 365, Google Workspace), CRM and marketing (Salesforce, HubSpot), infrastructure (AWS, Azure, Google Cloud), and AI services (OpenAI, Anthropic, Copilot, Gemini).

6.1 THREE GROUPS, THREE LEVELS OF URGENCY

DPF users: still formally legal. But the accountability principle (Art. 5(2) GDPR) requires you to assess the new situation and document a plan B. Under NIS2, the risk management obligation comes on top.[19]

SCC and BCR users: immediate action required. Your transfer impact assessments typically rely on the FTC, PCLOB, and DPRC as independent bodies. Those assumptions are void; the assessments must be updated without delay.[9][11]

Regulated industries: financial services, healthcare, critical infrastructure operators, and the public sector carry heightened documentation duties and reputational risks. For them, a documented contingency plan is not optional.[10]

6.2 THE AI FACTOR: TRANSFERS MISSING FROM THE RECORDS OF PROCESSING ACTIVITIES

Classic transfer inventories think in databases and file shares. AI systems, by contrast, generate personal data flows in real time: prompts containing customer and employee data, RAG contexts from internal documents, meeting transcripts, agent logs, and persistent “memories.” Important here: a “transfer” within the meaning of the GDPR does not require a physical data export. Remote access from a third country is enough.[10] If you run Copilot or US-hosted models in production, you almost always have more third-country transfers than your records of processing activities show.

6.3 WHAT KEEPS RUNNING EVEN IN THE WORST CASE

No panic on two fronts: non-personal data (pure machine, product, and telemetry data with no personal reference) is not covered by Chapter V of the GDPR. And Art. 49 GDPR permits necessary individual transfers, for instance for contract performance: the hotel booking in New York, the ticket with US support. What Art. 49 does not carry is the structural outsourcing of entire processing operations.[3]

THE PENALTY FRAMEWORK, SOBERLY CONSIDERED

Violations of the transfer provisions of Chapter V can draw fines of up to EUR 20 million or 4% of global annual revenue (Art. 83(5) GDPR). In practice, often more relevant than fines are prohibition orders from the supervisory authority, audit findings, contractual breaches toward customers, and exclusion from tenders with sovereignty requirements.

CONTRACTS REASSURE. ARCHITECTURE PROTECTS.

The reflexive answer to transfer risk is legal: more clauses, more annexes, more signatures. Necessary, but not sufficient. What holds when it counts are technical measures and an architecture in which providers are interchangeable.

LEGAL INSTRUMENTS: USING SCCS, TIAS, AND ART. 49 CORRECTLY

If the adequacy decision falls, data flows are not banned. Only the most convenient instrument goes away. The alternatives exist, but they demand real work: contracts plus assessment plus measures.

7.1 STANDARD CONTRACTUAL CLAUSES (SCCS)

The standard contractual clauses issued by the European Commission (Art. 46(2)(c) GDPR) contractually bind data exporter and importer to EU protection standards. They are the fallback instrument of choice. But since Schrems II, the rule is: SCCs alone are not enough. The exporter must examine whether the law of the destination country overrides the contractual commitments and, where necessary, adopt supplementary measures.[6][7]

A practical note that can save weeks: at the large US providers, SCCs are often already anchored as an automatic fallback in the data processing agreement (DPA), for example at Microsoft, Google, and AWS. The first step is therefore not a renegotiation but a review of what you have: Does the fallback kick in automatically if the DPF lapses? For which SCC modules? Are the annexes on the subject matter of processing and on technical and organizational measures fully completed?

7.2 TRANSFER IMPACT ASSESSMENT (TIA)

The TIA (also called a transfer risk assessment) documents this examination. In its Recommendations 01/2020, the European Data Protection Board describes a six-step approach:[7][20]

01 **Know your transfers:** record every transfer, including remote access and onward transfers to sub-processors.

02 **Identify the instrument:** adequacy decision, SCCs, BCRs, or a derogation under Art. 49?

03 **Assess effectiveness:** do the third country's access laws (FISA 702, CLOUD Act) override the instrument in practice?

04 **Adopt supplementary measures:** primarily technical measures (Chapter 08).

05 **Take formal steps:** update contracts and involve the supervisory authority where required.

06 **Reassess regularly:** without delay after relevant legal changes. Trump v. Slaughter is exactly such a change.

WHAT A TIA MUST CONTAIN AFTER JUNE 29, 2026

An honest reassessment names the facts: FTC independence struck down by the highest court, the PCLOB without a quorum since January 2025, the DPRC an executive body resting on a revocable order. If you pass over these facts in your assessment, you are not documenting diligence but its opposite, and in a dispute you are creating evidence against yourself.

7.3 BCRS AND ART. 49: THE EDGE SOLUTIONS

Binding Corporate Rules secure intra-group transfers but share the TIA problem: they too do not protect against government access in the destination country. The derogations of Art. 49 (consent, contract performance, legal claims) carry necessary individual cases but are explicitly unsuitable as a permanent solution for structural data flows.[3][20]

> **Legal instruments shift the risk onto paper. Whether the paper holds is decided by the technology behind it.**

TECHNICAL MEASURES THAT ACTUALLY HOLD

The European Data Protection Board is uncomfortably clear on this point: purely contractual and organizational supplementary measures do not, by themselves, create sufficient protection. As a rule, only technical measures that actually prevent access to personal data by recipients or authorities in the third country are effective.[7]

8.1 THE DIVIDING LINE: PLAINTEXT ACCESS

The decisive question is: can the US provider (or an authority acting through it) access plaintext? As soon as the recipient holds the plaintext or the key, it can be compelled to hand data over, and no contract clause in the world changes that.[7][21] This yields a clear sorting:

SETUP	ASSESSMENT UNDER EDPB LOGIC	STATUS
Backup/storage encrypted, keys held exclusively by the EU exporter	Effective: the importer sees only ciphertext; a government access request comes up empty (EDPB Use Case 1).	HOLDS
Pseudonymized processing, re-identification possible only in the EU	Effective if the importer cannot establish the personal reference and the additional knowledge remains in the EU.	HOLDS
Encryption in transit + encryption at rest at the US provider with the provider's keys	A mandatory baseline, but useless against government access: the provider can decrypt, so the provider can hand over.	FAILS
SaaS operation in plaintext (mail, CRM, office, AI assistant at the US provider)	EDPB Use Cases 6/7: for processing that requires plaintext access, no effective technical measures are known.	FAILS
EU data center of a US provider (“data residency”)	The CLOUD Act attaches to the provider's control, not to server location. Residency alone is cosmetics.[15][21]	FAILS

THE UNCOMFORTABLE CONSEQUENCE

For a large share of today's US SaaS usage, no technical measure exists that prevents the provider's plaintext access while keeping the service functional. Here, the only help is risk steering through data classification: what is allowed in at all? And architecture: how fast can I get out again?

THE TOOLBOX: TEN MEASURES RANKED BY IMPACT

01 Data minimization & classification
The cheapest measure first: what is not transferred does not need protection. Traffic-light classification (Ch. 09) before every new tool.

02 Pseudonymization before transfer
Replace direct identifiers with references (“customer-924” instead of a name); the mapping table stays in the EU. Recognized by the EDPB.

03 Tokenization
Field-level replacement of sensitive values, strong for CRM, ERP, health, and financial data. Detokenization only within the EU domain.

04 Encryption with EU key sovereignty
Customer managed keys are the minimum, bring your own key is better, hold your own key is strongest: keys sit physically beyond the provider's reach, for example in an EU HSM.

05 Client-side encryption
Encryption before upload; the provider never sees plaintext. Very strong, but functionally limited to storage and transport scenarios.

06 Confidential computing
Processing in trusted execution environments: data stays encrypted **even during computation**, and remote attestation proves the integrity of the environment. It closes the gap between “store encrypted” and “process in plaintext,” making it the key technology for AI workloads with sensitive data.[22]

07 Zero-retention configuration for AI
Ensure contractually and technically: no prompt storage, no training on your data, defined log retention periods, EU processing region.

08 Private deployments
Run open-weight models yourself (on-prem or in an EU VPC). Full control over data and weights, in exchange for operational responsibility.

09 Gateway instead of direct integration
The most important architecture decision, see below.

10 Exit capability as a design criterion
Open formats, documented export paths, contractual switching rights. The EU Data Act (fully applicable since September 12, 2025) obliges providers to make switching technically possible.[26]

8.2 THE GATEWAY ARCHITECTURE: MAKING MODELS INTERCHANGEABLE

If you build applications directly against the API of a single US provider, you chain your processes to that provider's legal situation. The resilient alternative inserts a control layer of your own:

```
APPLICATION → GATEWAY (AUTH · LOGGING · BUDGET)
            → POLICY LAYER (DATA CLASS · PII FILTER · ROUTING)
            → MODEL POOL (US API | EU API | LOCAL)
```

The effect: data classes decide the routing (sensitive content goes to EU-hosted or local models), every call is auditable, and if a legal basis falls, the affected endpoint is reconfigured instead of the application being rebuilt. A court ruling thus turns from an architecture problem into a configuration event.

THE 7-STEP PLAN FOR THE NEXT 12 MONTHS

Not a crisis program, but an approach from a position of strength: first transparency, then assessment, then rebuilding. Each step produces usable results on its own.

STEP	MEASURE	OUTCOME	HORIZON
01	**Inventory US exposure**	Transfer mapping from the records of processing activities: all SaaS, cloud, and AI services with a US nexus, with the legal basis per flow (DPF certification, SCCs, Art. 49). Include remote access and sub-processors.	WEEK 1–2
02	**Classify criticality**	Traffic-light model per data flow (see below). Prioritization: employee, health, financial, and customer data first.	WEEK 2–4
03	**Vendor due diligence**	A standardized question set for all US providers (page 17). Document the answers, put deadlines on the gaps.	WEEK 4–8
04	**Update TIAs**	Reassessment with the facts since June 29, 2026, and a documented risk decision by executive management. Especially for AI workloads.	WEEK 4–8
05	**Prepare the SCC fallback**	Review what exists first: with hyperscalers, the SCC fallback is often already anchored in the DPA (Ch. 7.1). For the remaining critical providers, have clause sets and annexes prepared and ready in the drawer, not negotiated in crisis mode.	MONTH 2–3
06	**Implement technical controls**	Ordered by leverage: key sovereignty, pseudonymization, gateway layer, confidential computing for sensitive AI workloads.	MONTH 3–9
07	**Anchor AI governance & exit**	A binding policy on which data classes may enter which AI systems; an exit strategy per core workload; integration into NIS2 risk management and management reporting.	MONTH 3–12

9.1 THE TRAFFIC-LIGHT MODEL FOR STEP 02

RED · STOP AND REVIEW

Personal, sensitive, or business-critical: health, HR, and financial data, trade secrets in prompts. Only with effective technical measures or an EU alternative.

YELLOW · CONDITIONAL

Personal, but limited: business contact data, processes that can be pseudonymized. Permissible with a documented TIA and supplementary measures.

GREEN · UNCRITICAL

No personal reference: machine data, public content, synthetic test data. Freely usable; document the classification anyway.

VENDOR QUESTION SET AND AI DATA RULES

9.2 TWELVE QUESTIONS FOR EVERY US PROVIDER

Ask them in writing and archive the answers. Evasive answers are themselves an audit finding.

01 Are you currently DPF-certified? What is your documented plan if the framework lapses?

02 Are signature-ready SCCs (mapped to modules) with all annexes available?

03 In which region is our data processed, not just stored?

04 Which group entities and sub-processors have technical access, and from which jurisdictions?

05 Do you offer CMK, BYOK, or HYOK? Where does the key material physically reside?

06 Do you support client-side encryption or confidential computing options?

07 For AI services: is zero retention available? Is exclusion from training contractually guaranteed?

08 How many government requests for EU customer data did you receive in 24 months? (transparency report)

09 Do you commit to challenging disclosure demands and informing us to the extent permitted?

10 Which export formats and paths exist for a complete data extraction?

11 What switching support do you provide under the EU Data Act, and at what cost?

12 Is there an EU operating company with its own infrastructure, or only a sales entity?

9.3 AI GOVERNANCE: THE FOUR-LINE POLICY AT THE CORE

The most effective AI data rule is the one every employee knows by heart. The core fits into four mappings; everything else is elaboration:

DATA CLASS	PERMITTED SYSTEMS
Green (no personal reference)	All approved AI services.
Yellow (limited personal data)	Only services with a documented TIA, EU region, and zero retention; pseudonymization before input.
Red (sensitive/critical)	Only EU-hosted or locally operated models, ideally behind your own gateway; plaintext never leaves the controlled domain.
Black (classified information, professional secrets)	No cloud AI. Exclusively dedicated, audited environments.

A PRACTICAL WARNING FROM FEBRUARY 2025

When the US government imposed sanctions on the chief prosecutor of the International Criminal Court in February 2025, he subsequently lost access to his Microsoft email account and switched to a Swiss provider. Microsoft explicitly disputed the characterization of a "blocking": it had at no point ceased services for the Court, and the separation of the account had been coordinated with the ICC.[23] Regardless of how the individual case is judged, the lesson stands: availability has a compliance dimension. If you run business-critical processes, you plan for loss of access, not just data leakage.

SOVEREIGN OPTIONS: A MARKET OVERVIEW

The market moved noticeably in 2025/2026: billions in investment, new offerings, and, with the European Commission's Cloud Sovereignty Framework (October 2025), for the first time an official assessment framework for procurement with sovereignty levels from SEAL-0 to SEAL-4.[24] The key is to cleanly distinguish three categories, because “sovereign” appears on very different labels.

CATEGORY	EXAMPLES	ASSESSMENT
EU-native providers (EU ownership, EU law, EU operations)	STACKIT (Schwarz Digits) · Open Telekom Cloud · IONOS · plusserver · Hetzner · OVHcloud · Nextcloud/collaboration	Clearest legal position, no CLOUD Act reach-through. Check feature coverage per workload; maturity is rising fast: Schwarz Digits is investing EUR 11 billion in an AI data center in Lübbenau, with the first construction phase due by the end of 2027.[28]
Trustee & key models (US technology, EU control)	T-Systems Sovereign Cloud (Google-based, key management by T-Systems) · Delos Cloud (SAP subsidiary, Microsoft-based, public sector: pilot operations, market entry 2026)	A compromise between functionality and control: operations or keys sit with an EU trustee, and the cloud operator has no access to the key material. Governance details decide the actual protective effect.[25][35]
Hyperscaler “sovereign” offerings (US ownership, EU packaging)	AWS European Sovereign Cloud (first region Brandenburg, since January 15, 2026) · Microsoft EU Data Boundary (completed 02/2025) · Google Sovereign Portfolio	Real progress on residency, personnel, and metadata. The jurisdiction conflict remains, however, as long as the parent company is subject to US law. Critics call it “sovereignty washing.”[21][29][30]

10.1 FEASIBILITY: THE NORTH HAS SHOWN THE WAY

That migration is not a theoretical concept is demonstrated by Schleswig-Holstein: according to the State Chancellery, by the end of 2025 almost 80 percent of the roughly 30,000 workstations in the state administration (outside the tax administration) were running LibreOffice instead of Microsoft Office, and the migration of around 44,000 email accounts to Open-Xchange was already complete. The state puts the saved license costs at more than EUR 15 million, against one-time switching costs of around EUR 9 million.[27] For mid-sized companies (German Mittelstand), the same mechanics apply at smaller scale: six to eighteen months per workload is a realistic planning figure, far cheaper than any emergency migration.

How large the gap between risk awareness and preparation is can be seen in a Lünendonk survey from March 2026 among IT leaders in the DACH region: 83 percent consider a kill-switch scenario, that is, the politically ordered shutdown of cloud services, fundamentally realistic. But only 57 percent have a documented exit strategy; 43 percent have none.[18]

10.2 THE RIGHT SEQUENCE

Not everything has to migrate. A tiered model carries further than maximal demands: move red workloads (Ch. 09) to EU-native or trustee models, leave yellow workloads where they are with key sovereignty and supplementary measures, and place green workloads by economics. Sovereignty comes from the ability to act, not from isolation.

THE STRATEGIC TAKEAWAY: ARCHITECTURE BEATS AGREEMENTS

Safe Harbor lasted fifteen years. Privacy Shield four. After three years, the DPF stands without a load-bearing rationale. If your only conclusion is to wait for the next agreement, you have not understood the pattern.

The real finding of this paper is uncomfortable and liberating at the same time: the stability of your data processing does not hang on decisions in Brussels, rulings in Washington, or the promises of individual providers. It hangs on decisions you make yourself: Which data leaves your control domain in plaintext? Who holds the keys? How fast can you replace a provider?

No contract answers these questions. Architecture does. And architecture, unlike transatlantic diplomacy, is entirely in your hands.

> **Data sovereignty does not mean giving up US technology. Data sovereignty means that a court ruling in Washington cannot stop your business.**

11.1 THREE PRINCIPLES FOR THE NEXT 24 MONTHS

Legal bases are weather. Architecture is climate. Build systems that treat a change of transfer basis as a configuration event, not a crisis project. Gateway layers, key sovereignty, and exit paths are the instruments for that.

Classification before technology. Most companies know more precisely which laptops they own than which personal data leaves through their AI tools. Transparency over data flows is the prerequisite for every further decision, and it can be established in weeks, not years.

Sovereignty is a portfolio, not a creed. Red workloads under EU control, yellow ones with technical guarantees, green ones by economics. If you sort this way, you use the innovation speed of the world market without chaining your fate to a foreign jurisdiction.

11.2 THE WINDOW

There is a rare moment in regulatory cycles: after the warning shot, before the impact. That is the moment we are in. The proceedings are pending, the arguments are on the table, the time horizons are known. Everything described in Chapter 09 can be implemented today calmly, at normal terms, and with a choice of providers. The same measures after a CJEU ruling cost a multiple and turn out worse under time pressure.

The companies that were prepared for Schrems II in 2020 did not have better lawyers. They had started earlier.

THE US EXPOSURE QUICK CHECK

Ten questions, answered honestly. Every “no” is one point. Keep count.

#	STATEMENT	YES	NO
01	We have a current inventory of all US services that process personal data.	☐	☐
02	The legal basis is documented for each of these data flows (DPF, SCCs, Art. 49).	☐	☐
03	Our transfer impact assessments have been reviewed since June 29, 2026.	☐	☐
04	We know which prompts, logs, and AI contexts leave our organization toward the US.	☐	☐
05	A binding rule exists on which data classes may enter which AI systems.	☐	☐
06	For our most sensitive data in US services, we hold the keys ourselves (BYOK/HYOK).	☐	☐
07	Signature-ready SCCs are in place for our critical US providers.	☐	☐
08	AI applications run through our own gateway layer, not directly against provider APIs.	☐	☐
09	A documented, tested exit option exists for every critical workload.	☐	☐
10	Executive management has made the residual-risk decision on US transfers in writing.	☐	☐

0–2 NO · SOLID

You belong to the prepared minority. Hold the line, watch the proceedings, and test your exit paths once a year.

3–5 NO · GAPS

The typical midfield: fundamentals in place, AI flows and key sovereignty open. Steps 01 to 04 of the plan close the most critical gaps in eight weeks.

6–10 NO · EXPOSED

A CJEU ruling would catch you unprepared, and so would a government data request. Start step 01 this week. Not out of fear, but because every week of head start becomes negotiating power later.

SOURCES

All sources last checked on July 3, 2026. Primary sources (courts, legislators, official bodies, corporate announcements) are listed ahead of the analyses and press reports.

PRIMARY SOURCES

[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 (in German). 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 (in German). schleswig-holstein.de

[28] Schwarz Digits: „Spatenstich in Lübbenau: Schwarz Digits investiert 11 Milliarden Euro in Europas digitale Souveränität", Pressemitteilung vom 17.11.2025 (in German). 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

STUDIES, ANALYSES, AND PRESS COVERAGE

STUDIES, ANALYSES, AND PRESS COVERAGE

[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 (in German). dsn-group.de

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

[11] Tagesspiegel Background: „US-Urteil bringt EU-US-Datentransfers unter Druck", 30.06.2026 (in German). 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 (in German). mrak.at

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

[14] Provectus: „US-Urteil zur FTC: Was Microsoft-Kunden jetzt prüfen sollten", 01.07.2026 (in German). 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) (in German). luenendonk.de

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

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

[22] Börse Express: „Datenschutz-Schock: US-Urteil gefährdet EU-Datenaustausch" (u. a. zur Rolle von Confidential Computing), 02.07.2026 (in German). 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 is the consultancy for secure AI transformation in mid-sized companies. We bring organizations into AI adoption in a controlled way: with a clear baseline assessment, resilient governance, and architectures that do not promise sovereignty but produce it. We translate regulation such as GDPR, the EU AI Act, and NIS2 into architecture and process decisions that work in day-to-day operations. No paper for the binder, but systems that survive audits and regulatory shocks.

KI-STANDORTBESTIMMUNG (AI BASELINE ASSESSMENT)

The structured entry point: an AI operational readiness check across five dimensions (data access, model risk, process maturity, governance, security) with traffic-light scoring, a risk and governance analysis, and a 30/60/90-day roadmap. The US exposure mapping of steps 01 to 04 from Chapter 09 is part of the risk analysis here.

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

SICHERES KI-TRANSFORMATIONSPROGRAMM (SECURE AI TRANSFORMATION PROGRAM)

The modular implementation: AI hardening & resilience (guardrails, PII masking, auditability, failover), infrastructure design with gateway architecture and key sovereignty, enablement for your teams. Exactly the measures from Chapter 08, built for your operations.

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

Let's talk about your exposure before a court does.

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