EU-US Data Transfers After the Supreme Court's FTC Ruling: What It Means for Your Meeting Data

The Supreme Court's FTC ruling weakened the legal basis for EU-US data transfers. What it means for the Data Privacy Framework, SCCs, and your meeting data.

Published by Julian Pscheid · July 2, 2026
Read this article online: https://www.hedy.ai/post/eu-us-data-transfers-supreme-court-ftc-ruling/

A European professional reviewing documents at a desk with the EU flag and a data-privacy hologram in warm light

Quick answer On June 29, 2026, the US Supreme Court ruled in Trump v. Slaughter that the Federal Trade Commission no longer has to be independent. EU law requires an independent privacy watchdog in any country it sends personal data to, and the EU-US Data Privacy Framework leaned on the FTC's independence to clear that bar. Nothing changes overnight, because the framework stays valid until the European Commission or the EU courts strike it down. But the legal ground under EU-US transfers has shifted, and companies that rely on Standard Contractual Clauses need to revisit their paperwork. If you use Hedy, the parts that matter most already avoid a US transfer: speech recognition runs on your device, and EU-region users get storage and AI processing inside Europe.

Our GDPR consultant flagged this the morning the decision landed. It is worth understanding rather than reacting to, and the short version is simple: the ruling matters for EU-US data transfers, but nothing has switched off yet.

At a glance

Mechanism	Status after the ruling	What to do
EU-US Data Privacy Framework	Legally valid for now, but its legal foundation is undermined	Plan for a possible Commission withdrawal or a court challenge over the next two to three years
Standard Contractual Clauses (SCCs)	Still a valid mechanism, but harder to justify honestly	Update your Transfer Impact Assessment now
Transfer Impact Assessments (TIAs)	Must now account for a US supervisor that is no longer independent	Redo them, starting with your most sensitive data
Hedy on-device transcription	Unaffected: the audio never leaves your device	Nothing, it works this way by default
Hedy local AI inference	Unaffected: the analysis also runs on your device, so nothing is sent anywhere	Turn on Local AI Processing (optional, off by default)
Hedy EU data residency	No transatlantic transfer: your data is stored on EU servers and inference runs in the EU	Choose the EU region at signup

What the Supreme Court actually decided

On June 29, 2026, the Supreme Court decided Trump v. Slaughter (https://www.scotusblog.com/2026/06/court-allows-trump-to-fire-ftc-commissioner-and-overturns-major-restraint-on-presidential-power/) by a 6-3 vote. The Court held that the President could remove Federal Trade Commission member Rebecca Slaughter without cause, and in doing so it overruled Humphrey's Executor , a 1935 precedent that had let Congress shield the heads of certain agencies from being fired at will.

The effect is direct. FTC commissioners now serve at the President's pleasure. The agency that Congress designed to be bipartisan and independent is, in constitutional terms, no longer independent of the executive branch.

Why a US ruling reaches your EU data

On its face this is a case about presidential power, not privacy. The connection runs through EU law.

When the EU decides a non-EU country protects personal data well enough to receive it without extra safeguards, it issues an "adequacy decision." One requirement is that the country has an independent authority supervising data protection. The EU-US Data Privacy Framework, adopted in July 2023, is that adequacy decision for the United States, and the European Commission relied on the FTC's independence 259 times when it made the call. The same logic reaches the Data Protection Review Court and the Privacy and Civil Liberties Oversight Board, the other US bodies the framework treats as independent checks.

Remove the independence and the foundation the Commission built on starts to look unstable. As noyb (https://noyb.eu/en/us-supreme-court-just-blew-eu-us-data-transfers) put it, the reasoning that supported the whole arrangement no longer holds.

What it means for the mechanisms companies rely on

Three things are worth keeping separate.

The Data Privacy Framework is not gone. It stays legally valid until the European Commission withdraws it or the EU Court of Justice annuls it. noyb, the group led by Max Schrems, has already asked the Commission to withdraw it in an orderly way and says it will take the question to court. A ruling could take two to three years. This is the path that ended Safe Harbor in 2015 and Privacy Shield in 2020, so a third invalidation belongs in your planning, not in the footnotes.

Standard Contractual Clauses come with a catch. SCCs are the backup most companies fall back on, but they only work if you also run a Transfer Impact Assessment showing the destination country protects the data in practice. That assessment now has to account for a supervisory authority that is no longer independent.

Carsten Wittmann (https://tumaki.de) , a GDPR and AI-compliance consultant who advises Hedy (https://trust.hedy.ai) on its data-protection work, put the problem plainly:

> *Without an independent FTC, you no longer can come to the conclusion that all the required criteria are met.*

The advice at this stage is measured, not alarmed. Update your Transfer Impact Assessments now, map where your data goes, and start with your most sensitive processing, but do not abandon a framework that is still in force. The mistake after Schrems II was waiting until the last moment and then improvising.

Where Hedy stands, honestly

We would rather be straight about this than pretend Hedy sits outside the problem. Hedy's US-region path uses the same EU Standard Contractual Clauses (Module 2) and Transfer Impact Assessment that the rest of the industry uses, and that path is affected by this ruling like any other. The full framework, including our DPA, SCCs, TIA, and technical measures, is documented in our GDPR compliance post (/post/hedy-ai-gdpr-compliance/) and our Trust Center.

What sets Hedy apart is not a cleverer contract. It is that two parts of how Hedy works never depend on a US transfer decision at all.

The two things that don't depend on a transfer decision

On-device speech recognition. Hedy transcribes your conversation on your own phone, tablet, or computer. The audio, the most sensitive part of any meeting, becomes text on hardware you control and is never sent to a server to be transcribed. It works the same way on every platform Hedy supports. No transfer, to the US or anywhere else, happens for that step. As Carsten put it, "local processing on device is always possible." Hedy can take that further on supported devices: with Local AI Processing turned on, the AI analysis runs on your device as well, so nothing about the conversation is sent anywhere at all.

EU data residency with EU inference. When you choose the EU region, your conversation data is stored on European servers, and every part of the AI analysis runs on infrastructure inside the EU. We can guarantee that: for EU-residency accounts, inference never leaves Europe. Our primary inference provider, Nebius, is itself a European company, Netherlands-domiciled and running in EU data centers. For resilience we keep failover capacity with a few other providers that also run their inference inside the EU, though those companies are US-headquartered. Either way, your conversations are analyzed in Europe rather than shipped across the Atlantic. You can read the full picture in our EU data residency post (/post/eu-data-residency/) .

This addresses a fair objection Carsten raises. Where your data is processed is the first question, and for EU-residency accounts the answer is always Europe. Who operates that processing is the second. EU data residency run entirely by a US company lowers the risk without fully removing it, because a US parent can still be reached by US law. Having a European company as our primary provider is the strongest version of the answer, with US-headquartered providers kept only as EU-based failover.

Two honest caveats. A few operational services, including account login, billing, and error reporting, still run through US infrastructure for everyone, and none of them carry your conversation content. Session recap emails are the exception: they include your session summaries and notes, and they go out through US-based email infrastructure, so if that matters to you, you can switch them off and read your recaps in the app instead. And existing users on the US region stay there until they move; the European setup applies to the EU region.

What EU businesses should do now

Carsten's guidance (https://www.linkedin.com/feed/update/urn:li:activity:7478464182837817345/) , which matches the consensus among data-protection lawyers, is to treat the framework falling as a scenario to prepare for rather than a risk to hope away.

1. Inventory your transfers. List which providers hold personal data in the US, for what, and on what legal basis.
2. Update your Transfer Impact Assessments. Reflect the fact that US oversight is no longer independent, and document your reasoning.
3. Start with sensitive data. Health, financial, employee, and minors' data first.
4. Weigh EU-based alternatives at each renewal. You do not have to rip everything out today, but every new contract is a chance to reduce exposure.

For a buyer-side view of how to evaluate meeting tools specifically, our GDPR checklist for AI meeting tools (/post/gdpr-checklist-ai-meeting-tools/) and our comparison of GDPR-compliant AI meeting tools (/post/best-gdpr-compliant-ai-meeting-tool-record-transcribe-eu-data-protection/) walk through what to look for.

What is still uncertain

Two outcomes could change the picture. The European Commission could read the "independent authority" requirement less strictly, though that would be an awkward reversal of its own standard. Or the US position could shift over time. Neither is likely soon, and both would take years to play out. Until then, the honest description is uncertainty, not resolution, which is exactly why architecture that avoids the transfer is worth more right now than a contract that papers over it.

The bottom line

The ruling did not switch anything off, but it moved the ground under EU-US data transfers, and the direction of travel is clear. The durable protections are the ones that never send your data across the Atlantic in the first place. With Hedy, speech recognition stays on your device, and EU-region users keep both storage and AI processing inside Europe.

Update to the latest version and choose the EU region during onboarding, or lean on on-device processing wherever you are. Full compliance documentation is in our Trust Center at trust.hedy.ai (https://trust.hedy.ai) .

Frequently asked questions

Does the Supreme Court ruling make EU-US data transfers illegal?

No. The EU-US Data Privacy Framework stays legally valid until the European Commission withdraws it or the EU Court of Justice annuls it. The ruling weakens the legal foundation the framework was built on, but nothing changes overnight. Companies that rely on Standard Contractual Clauses should update their Transfer Impact Assessments now rather than wait for a court to force the issue.

Is the EU-US Data Privacy Framework dead?

Not yet. The framework remains in force. noyb, run by Max Schrems, has asked the European Commission to withdraw it in an orderly way and plans to challenge it in court, which could take two to three years. This is the same path that ended Safe Harbor in 2015 and Privacy Shield in 2020, so a third invalidation is a scenario worth planning for.

Do Standard Contractual Clauses still work after this ruling?

SCCs are still a valid transfer mechanism, but they only hold up if your Transfer Impact Assessment shows the destination country protects the data in practice. With the FTC no longer independent, that assessment is harder to complete honestly for transfers to the US. Update your TIAs to reflect the change and prioritize sensitive data.

Does this ruling affect my Hedy data?

The parts of Hedy that matter most avoid a US transfer entirely. Speech recognition runs on your own device, so your audio is never sent anywhere to be transcribed. If you choose the EU region, your conversation data is stored in Europe and the AI analysis runs on infrastructure inside the EU. Hedy's US-region path uses SCCs and a Transfer Impact Assessment like most tools, so it is affected like the rest of the industry.

What should EU businesses do right now?

Take a staggered approach: inventory where your data goes, update your Transfer Impact Assessments, start with your most sensitive processing, and weigh EU-based alternatives at each contract renewal. Treat the framework falling as a scenario to plan for, not a tail risk. Companies that waited after Schrems II ended up improvising against a deadline.
