Analysis · May 18, 2026

← Previous·Next →

Schrems II, five years on

The ruling that changed the law on international transfers of personal data. Five years on, a considerable part of daily European office life continues to operate as if nothing had happened.

The ruling that took three hours to change the rules

On July 16, 2020, around a quarter past ten in the morning Luxembourg time, the Court of Justice of the European Union made public the ruling in Case C-311/18. In the following three hours, the legal regime that supported the daily transfer of personal data from Europe to the United States —the so-called Privacy Shield— ceased to exist. By the time European data protection officers finished lunch that day, the framework under which their companies and administrations operated was no longer valid.

The ruling is known today as Schrems II, named after Maximilian Schrems, the Austrian activist whose complaint against Facebook Ireland triggered it. The complaint, specifically, dealt with transfers between Facebook Ireland and Facebook United States. The ruling, in general, goes much further: it dictates how and under what conditions any personal data collected on European territory can pass to the United States.

Almost six years later, the replacement framework exists —the EU-US Data Privacy Framework, adopted in July 2023— and is also under legal pressure. A new Schrems round is in the works. Meanwhile, European small and medium-sized enterprises continue to use US cloud services for everyday tasks, for the most part without knowing that the legal issue on which those services rest remains open.

What exactly Schrems II said

The ruling rests on three pieces. The first is the Charter of Fundamental Rights of the European Union, in particular its Articles 7 (private and family life), 8 (protection of personal data), and 47 (right to an effective remedy and to a fair trial). The second is the General Data Protection Regulation —the GDPR that many Europeans only remember for cookie notices—, specifically its Chapter V, Articles 44 to 50, on international transfers. The third is US intelligence legislation: Section 702 of the Foreign Intelligence Surveillance Act, FISA 702 in legal jargon, and presidential Executive Order 12333.

The court proceeded by contrast. The Charter of Fundamental Rights requires that the personal data of European citizens enjoy, when they leave the Union, a level of protection essentially equivalent to that guaranteed by the GDPR. The question was, consequently, whether the United States offers that essentially equivalent level.

The answer was negative, and not because of nuances. FISA 702 allows the US government to collect communications of non-US persons located outside the national territory without prior individual judicial authorization, without notification to the affected party, and without an effective remedy comparable to the European one. Executive Order 12333 analogously expands that capacity outside the national territory. The court concluded that the European citizen, before the US legal system, does not have the essentially equivalent protection that the Charter requires. Equivalence, therefore, does not exist.

Hence the direct consequence: European Commission Decision 2016/1250, which had validated the Privacy Shield as an adequate framework for transfers, was declared invalid. Every transfer covered solely by that framework was left without a legal basis from that very moment.

What did survive (and under what conditions)

Schrems II did not eliminate all instruments. Standard Contractual Clauses —SCC in international jargon— survived. They are model contracts approved by the European Commission: a European exporter and an importer from the destination country sign them, committing to treat the data according to the European standard. The company that thought it had solved the problem on July 17, 2020, signed SCCs with its provider and was satisfied.

The discomfort came when reading the sentence slowly. The court made it clear that the SCCs remain valid, but their validity depends on a condition that should be underlined: that the importer of the data can comply with them in practice. If the national legislation of the destination country prevents it from complying with the clauses —because, for example, an order under FISA 702 forces it to hand over the data without notifying its European counterpart—, the clauses do not really protect. And then, says the court, the European exporter must suspend the transfer.

This introduced a new object into European data protection practice: the Transfer Impact Assessment, known by its acronym TIA. Every time a European company wants to transfer data to the United States under the cover of SCC, it must formally evaluate whether the recipient can comply with the clauses given the legislation applied to it. The European Data Protection Board (EDPB) published detailed guidelines on how to conduct the TIA. Honest practice usually yields the same result: if the importer is a US subsidiary of a cloud giant, the sincere answer to the TIA is that the clauses cannot be fulfilled as they are written.

The Privacy Framework and the pending Schrems III

On July 10, 2023, the European Commission adopted a new Adequacy Decision: 2023/1795. It replaces the defunct Privacy Shield and operates under the name EU-US Data Privacy Framework. The United States previously modified its internal regime through Executive Order 14086, which limits the scope of signals intelligence to what is "necessary and proportionate" —terminology familiar to the European reader, not so much to US administrative practice— and creates a review body called the Data Protection Review Court (DPRC). The Commission considered that these modifications were sufficient to restore the essentially equivalent level of protection.

The organization noyb, founded by Schrems, filed a complaint on September 7, 2023, against the new Decision. The arguments are as expected: the DPRC is not an independent court in the sense of Article 47 of the Charter; the concepts of "necessary and proportionate" do not mechanically translate European standards; and, finally, a protection that rests on an Executive Order can be revoked by the following Executive Order. A CJEU ruling on the new Decision —what many already call, with some resignation, Schrems III— is expected in the coming years. The result cannot be anticipated. The structure of the argument, in any case, is very reminiscent of that of 2020.

What the European SME does not hear

While the Grand Chamber of the CJEU deliberates, the medium-sized law firm continues to exchange correspondence with its clients through Microsoft 365 hosted in European regions but owned by a US company subject to FISA 702. The private medical practice synchronizes agendas through Google Workspace. The tax advisor sends signed returns via DocuSign. The psychologist invoices from a spreadsheet in Notion. The labor law firm archives files in Dropbox. And practically all of them, moreover, serve their clients via WhatsApp. All

of this can operate under the cover, according to the providers, of the Adequacy Decision 2023/1795. The day that Decision falls in Schrems III, all those relationships are left in the open in the same second.

The issue is not rhetorical. Between 2022 and 2024, several European authorities resolved cases against data controllers for using Google Analytics without an adequate transfer instrument, in literal application of the CJEU's reasoning even before the Privacy Framework entered into force. The French authority, the CNIL, was the first to formalize the criterion in 2022; the Austrian, Italian, and other authorities followed shortly after. Non-compliance, under the current operational design of the European SME, is documented in real time before whoever knows how to look.

The TIA as an instrument, not a ritual

A considerable part of the TIAs circulating through European offices are, when read carefully, formal exercises. They list contractual instruments, enumerate the provider's certifications, cite technical guarantees, check the box. Few seriously ask if a FISA 702 order would force the provider to hand over the data. Even fewer ask what would happen to that transfer under a hypothetical review of the Privacy Framework. Article 5 of the GDPR requires the data controller to be able to demonstrate compliance. A TIA that is not done seriously demonstrates nothing; what it demonstrates is the will to comply on paper while doing the opposite in practice.

The sincere version of the TIA starts with a simple question: what would happen if tomorrow a FISA 702 order arrived at this provider for these specific data? If the honest answer is "they would have to hand them over without notifying us," the contractual clauses do not solve the problem. What does solve it, in cases where the question really matters, is not having put the data in the hands of that provider.

Political change as structural risk

There is an additional layer, political, that is worth naming without drama. Adequacy Decision 2023/1795 rests, in the final analysis, on Executive Order 14086, signed by President Biden in October 2022. An Executive Order is signed by one president and can be revoked, modified, or emptied of content by the next. The protection of European data in the United States thus depends on an administrative decision that neither the American Congress guarantees nor the American legal system protects with the solidity with which it protects other internal matters. Since January 2025 a new administration has been governing the United States, and the question about the practical continuity of EO 14086 has ceased to be a hypothesis and has become contemporary. Any scenario in which the administration decides to withdraw or attenuate the Order would leave the European Decision without the piece on which it was built.

It is not a conspiracy argument. It is a sober reading of the legal design. Transatlantic data protection frameworks have already fallen twice: Safe Harbor in 2015 (Schrems I ruling), Privacy Shield in 2020 (Schrems II). The third rests on a more fragile piece than its two predecessors. A European company that today bets its data processing on that piece is making a risk management decision, not a mere regulatory compliance decision.

For the professional reader

The operational questions that it is worth asking oneself before choosing a cloud service for professional data — with the rigor with which a data protection inspector would pose them— are the following:

1. Where is the data physically stored? A European region is not a sufficient answer if the operator is American.
2. Who operates the service, in what jurisdiction is it incorporated, and what legal orders can it be subjected to?
3. What transfer instrument is invoked: Adequacy Decision 2023/1795, SCC with TIA, derogation from Article 49 of the GDPR? Is that choice defensible before an inspection?

4. If the Adequacy Decision were to fall tomorrow, what operational plan exists to maintain activity?
5. Is there a European or self-hosted alternative for that function, and what would be the real cost of migrating?

Not all daily office functions require the same response. A spreadsheet for internal accounting probably does not raise the question to this level. A client's criminal file, medical history, employee payroll, do. Proportionality is legitimate; the collective inertia with which the European SME has remained with US providers for everything —even for the most sensitive— is not.

Schrems II turns six this July. The ruling has not changed the daily habits of most European companies. It has, however, changed the risk map to which those companies are exposed. When a US administrative decision stands between European regulation and the actual operation of an SME, it is worth at least knowing that the decision is there, and that it is fragile. Those of us who have chosen an architecture without an operator in the middle — the thread that runs through Cuadernos Lacre— would prefer not to have to write this kind of analysis every time a Schrems sits down to file an appeal. But we will continue to do them.

Sources and further reading

- Court of Justice of the European Union — judgment of July 16, 2020, Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*.
- Regulation (EU) 2016/679, Chapter V, Articles 44 to 50 — international transfers of personal data.
- Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequate level of protection of personal data under the EU-US Data Privacy Framework.
- European Data Protection Board — *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, adopted on 18 June 2021.
- noyb.eu — complaint filed on September 7, 2023, against Decision (EU) 2023/1795 before the European data protection authorities.
- *Foreign Intelligence Surveillance Act*, Section 702 (codified at 50 U.S.C. § 1881a), and Executive Order 12333 on US intelligence activities outside national territory.

← PreviousWhen no one is in betweenNext →CUADERNOS_LIST_SHA256_TITLE

Recent readings

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Take this article wherever you need it.

↓ Markdown ↓ Plain text ↓ PDF

The file is downloaded to your device. From there, you can save it, import it into Solo2, or share it as you wish. Cuadernos does not decide the destination for you.

Wax seal · SHA-256 06e3c83a000efc6139253df04b3a1ee0833942e5502ae3a3644673e94fb69782

Cuadernos Lacre · A publication of Menzuri Gestión S.L. ·
written by R.Eugenio · edited by the team of Solo2.