分析 · 2026 年 5 月 18 日

← 上一页·下一页 →

Schrems II，五年后

改变国际个人数据传输法律的判决。五年后，欧洲大部分日常办公运作依然如故。

通俗地说： 2020年7月16日的一个周四上午，一家欧洲法院宣布，公司向美国发送你数据的大部分方式都是非法的。五年后的今天，几乎没人做出改变。你的信息仍然像那时一样在空中飞过。

仅用三小时便改变规则的判决

2020 年 7 月 16 日，卢森堡时间上午 10 点 15 分左右，欧盟法院公布了 C-311/18 案的判决。在接下来的三小时内，支撑欧洲向美国日常传输个人数据的法律机制——即所谓的隐私盾（Privacy Shield）——不复存在。当那天欧洲的数据保护官们吃完午饭时，他们的公司和行政部门赖以运作的框架已经失效了。

该判决如今被称为 Schrems II，以奥地利活动家 Maximilian Schrems 的名字命名，他针对 Facebook Ireland 的申诉触发了这一判决。具体而言，该申诉关注 Facebook 爱尔兰与 Facebook 美国之间的传输。概括而言，该判决影响更为深远：它规定了在欧洲领土上收集的任何个人数据可以如何以及在何种条件下传输到美国。

近六年后，替代框架已经存在——即 2023 年 7 月通过的 EU-US Data Privacy Framework——且同样面临法律压力。新一轮的 Schrems 正在酝酿中。与此同时，欧洲中小企业继续在日常任务中使用美国的云服务，大部分人并不知道这些服务赖以存在的法律问题仍然悬而未决。

Schrems II 究竟说了什么

该判决建立在三个基石之上。第一是《欧盟基本权利宪章》，特别是其第 7 条（私人和家庭生活）、第 8 条（个人数据保护）和第 47 条（有效司法保护）。第二是《通用数据保护条例》——许多欧洲人仅通过 Cookie 提示记住的 GDPR——特别是其第五章，关于国际传输的第 44 至 50 条。第三是美国的法律情报立法：《外国情报监视法》（Foreign Intelligence Surveillance Act）第 702 条，法律术语为 FISA 702，以及总统第 12333 号行政命令。

法院通过对比进行裁决。《基本权利宪章》要求欧洲公民的个人数据在离开欧盟时，必须享有与 GDPR 所保障的基本等同的保护水平。因此，问题在于美国是否提供了这种基本等同的水平。

回答是否定的，且并非因为细微差别。FISA 702 允许美国政府在没有事先获得个人司法授权、没有通知当事人且没有与欧洲相当的有效救济手段的情况下，收集位于国境外的非美国人的通信。第 12333 号行政命令在国境外以类似方式扩大了这种能力。法院得出结论，欧洲公民在美国法律体系面前不享有《宪章》所要求的实质上等同的保护。因此，等同性并不存在。

由此产生的直接后果是：欧盟委员会第 2016/1250 号决定（该决定曾验证隐私盾作为传输的适当框架）被宣布无效。从那一刻起，所有仅依赖该框架的传输都失去了法律依据。

幸存下来的内容（及在何种条件下）

Schrems II 并未取消所有工具。标准合同条款——国际术语为 SCC，英文缩写为 Standard Contractual Clauses——幸存了下来。它们是欧盟委员会批准的合同模板：欧洲出口方与目的地国的进口方签署这些条款，承诺按照欧洲标准处理数据。在 2020 年 7 月 17 日认为问题已解决的公司，与供应商签署了 SCC 并感到心满意足。

在仔细阅读判决书时，不安随之而来。法院明确指出 SCC 仍然有效，但其有效性取决于一个需要强调的条件：数据进口方能够在实践中履行这些条款。如果目的地国的国家立法阻碍其履行条款——例如，根据 FISA 702 的指令强制其交付数据而不通知其欧洲对应方——那么这些条款实际上并没有起到保护作用。法院表示，在这种情况下，欧洲出口方必须暂停传输。

这在欧洲数据保护实践中引入了一个新对象：传输影响评估（Transfer Impact Assessment），英文缩写为 TIA。每当欧洲公司希望在 SCC 的保护下将数据传输到美国时，必须根据接收方适用的法律正式评估其是否能够履行条款。欧洲数据保护委员会（EDPB）发布了关于如何进行 TIA 的详细指南。诚实的实践通常会得出同样的结果：如果进口方是美国云巨头的子公司，那么对 TIA 的坦诚回答是，这些条款无法按照书面要求履行。

Privacy Framework 与待定的 Schrems III

2023 年 7 月 10 日，欧盟委员会通过了一项新的充分性决定：2023/1795。它取代了已失效的隐私盾，并以欧盟-美国数据隐私框架（EU-US Data Privacy Framework）的名义运作。美国此前通过第 14086 号行政命令（Executive Order）修改了其内部机制，将信号情报的范围限制在“必要且适度”的范围内——这对欧洲读者来说是熟悉的术语，但在美国行政实践中并非如此——并创建了一个名为数据保护审查法院（DPRC）的审查机构。委员会认为这些修改足以恢复基本等同的保护水平。

由 Schrems 创立的 noyb 组织于 2023 年 9 月 7 日对新决定提起申诉。论据如预期所料：DPRC 并不是《宪章》第 47 条意义上的独立法院；“必要且适度”的概念并不能机械地转化欧洲标准；最后，基于行政命令的保护可以被下一项行政命令撤销。欧盟法院对新决定的判决——许多人已带着某种无奈将其称为 Schrems III——预计将在未来几年内做出。结果无法预料。无论如何，论证结构与 2020 年非常相似。

欧洲中小企业未曾察觉的真相

在欧盟法院大法庭审理期间，中型律师事务所继续通过托管在欧洲区域但归属于受 FISA 702 管辖的美国公司的 Microsoft 365 与客户交换信件。私人医疗咨询通过 Google Workspace 同步日程。税务顾问通过 DocuSign 发送签署的声明。心理学家从 Notion 的电子表格中开具发票。劳动律师事务所在 Dropbox 中存档案卷。而且几乎所有人都在通过 WhatsApp 服务客户。根据供应商的说法，所有这些都可以在 2023/1795 充分性决定的保护下运作。一旦该决定在 Schrems III 中失效的那天，所有这些关系将在同一秒内暴露在风险之中。

这并非修辞问题。2022 年至 2024 年间，多个欧洲机构裁定了针对数据控制者在没有适当传输工具的情况下使用 Google Analytics 的案卷，即使在 Privacy Framework 生效之前，也字面上应用了欧盟法院的逻辑。法国机构 CNIL 在 2022 年率先将该标准正式化；奥地利、意大利等机构紧随其后。在欧洲中小企业目前的运营设计下，对于知道往哪看的人来说，违规行为正被实时记录。

作为工具而非仪式的 TIA

在欧洲办公室流传的大量 TIA，如果仔细阅读，其实是形式化的练习。它们列出合同工具、枚举供应商的认证、引用技术保证、勾选选项框。很少有人认真询问 FISA 702 指令是否会强制供应商交付数据。更少有人询问在假设的 Privacy Framework 修订下，这种传输会发生什么。GDPR 第 5 条要求数据控制者能够证明其合规性。不认真做的 TIA 证明不了任何事情；它证明的只是在实践中反其道而行之的同时，在纸面上满足合规要求的意愿。

坦诚版本的 TIA 从一个简单的问题开始：如果明天这家供应商收到一份关于这些特定数据的 FISA 702 指令，会发生什么？如果诚实的回答是“他们必须在不通知我们的情况下交付数据”，那么合同条款并不能解决问题。在问题真正重要的情况下，真正能解决问题的是不要将数据交到该供应商手中。

作为结构性风险的政治变动

还有一个额外的政治层面，值得在不带戏剧色彩的情况下提及。2023/1795 充分性决定最终建立在拜登总统于 2022 年 10 月签署的第 14086 号行政命令之上。行政命令由一位总统签署，可以被下一位总统撤销、修改或架空。因此，欧洲数据在美国的保护取决于一项行政决定，既没有美国国会的保障，美国法律系统对其保护的稳固性也不如保护其他内部事务。自 2025 年 1 月起，新一届政府治理美国，关于 EO 14086 实践连续性的问题已不再是假设，而是变成了现实。任何政府决定撤回或削弱该命令的情形，都会让欧洲的决定失去其赖以建立的基石。

这并非阴谋论，而是对法律设计的冷静解读。跨大西洋数据保护框架已经崩溃过两次：2015 年的 Safe Harbor（Schrems I 判决），2020 年的 Privacy Shield（Schrems II）。第三个框架建立在一个比前两个更脆弱的基石上。今天将数据处理押在这个基石上的欧洲公司是在做出风险管理决定，而非仅仅是法规合规决定。

致专业读者

在为专业数据选择云服务之前，值得提出的操作性问题——以数据保护监察员会提出的那种严谨度——如下：

1. 数据物理存储在何处？如果运营商是美国的，那么“欧洲区域”并不是一个充分的答案。
2. 谁在运营该服务，它在哪个司法管辖区注册，以及它可能服从哪些法律指令？
3. 援引了哪种传输工具：2023/1795 充分性决定、带有 TIA 的 SCC，还是 GDPR 第 49 条的豁免？这种选择在审计时是否站得住脚？
4. 如果充分性决定明天失效，现有的维持业务运行的操作计划是什么？
5. 该功能是否有欧洲或自托管的替代方案，迁移的实际成本是多少？

并非所有日常办公功能都需要同样的回答。用于内部会计的电子表格可能不会将问题提升到这个层面。但客户的刑事案卷、病史、员工工资单则会。比例原则是合理的；而欧洲中小企业在所有事情上——甚至是处理最敏感的数据时——都依赖美国供应商的集体惯性是不合理的。

Schrems II 裁决到今年 7 月就满六年了。这项判决并未改变大多数欧洲公司的日常习惯，但它确实改变了这些公司所面临的风险版图。当美国的一项行政决定介入欧洲法规与中小企业的实际运营之间时，至少应该知道该决定的存在，并且它是脆弱的。我们中那些选择了无中间运营商架构的人——这也是贯穿 Cuadernos Lacre 的主线——更希望不必在每次 Schrems 提起诉讼时都撰写此类分析。但我们会继续写下去。

编者按： 当本 Cuadernos 提及公司或产品名称时，并非为了指责。这些产品的开发者所做的工作被数百万人使用和欣赏。我们指出的是结构性问题——是模式问题，而非品牌问题。品牌作为例子出现，是因为读者熟悉它们。

来源及延伸阅读

- 欧盟法院——2020 年 7 月 16 日判决，案件号 C-311/18，*数据保护专员诉 Facebook Ireland Ltd. 和 Maximillian Schrems*。
- （欧盟）2016/679 号法规，第五章，第 44 至 50 条——个人数据的国际传输。
- 委员会 2023 年 7 月 10 日发布的（欧盟）2023/1795 号执行决定，关于 EU-US Data Privacy Framework 框架下个人数据保护的充分水平。
- 欧洲数据保护委员会——*关于补充传输工具以确保符合欧盟个人数据保护水平的措施的第 01/2020 号建议*，于 2021 年 6 月 18 日通过。
- noyb.eu——2023 年 9 月 7 日向欧洲数据保护机构提交的针对（欧盟）2023/1795 号决定的申诉。
- 《外国情报监视法》（*Foreign Intelligence Surveillance Act*）第 702 条（编纂于 50 U.S.C. § 1881a），以及关于美国境外情报活动的第 12333 号行政命令。

← 上一页当中间没有任何人时下一页 →SHA-256 究竟是什么

最近阅读

- 分析 · 2026年5月18日 真实隐私 vs 表象隐私：你应该问自己的问题

- 分析 · 2026年5月18日 作为专业实践的自托管 (Self-hosting)
- 概念 · 2026年5月18日 24 个单词：什么是加密身份

随身携带本文，以备不时之需。

↓ Markdown ↓ 纯文本 ↓ PDF

文件将下载到您的设备中。您可以从那里将其保存、导入 Solo2 或在任何地方共享。Cuadernos 不会为您决定文件的去向。

火漆印章 · SHA-256 e92975ffcf1a6d9584477decc71321f0c005aba025ad03a02e672e814f5ccd4c

Cuadernos Lacre · Menzuri Gestión S.L. 的出版物 ·
由 R.Eugenio 撰写 · 由 Solo2 团队编辑。