ANONOS

How Cloud, SaaS and Outsourced Data Processing Can Remain Lawful After the Schrems II Invalidation of the Privacy Shield for International Data Transfers

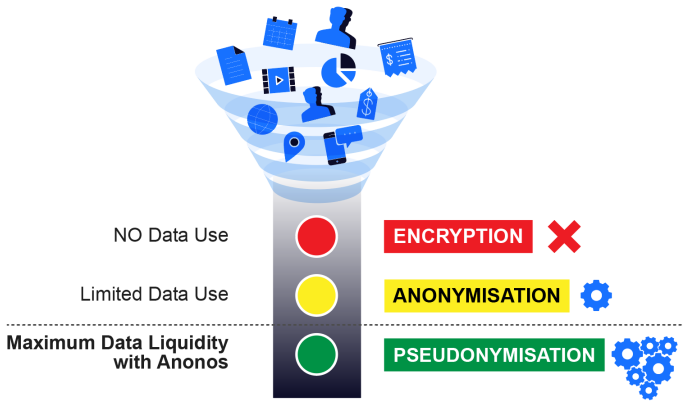
The biggest development in years impacting international data processing was the recent invalidation of the Privacy Shield by the Court of Justice of the European Union in the "Schrems II" court decision.[1]

Companies that previously relied on the Privacy Shield for the processing of EU personal data, including cloud, SaaS and outsourcing arrangements, now need a new legal basis for the processing to remain lawful.[2]

To date, the only EU data protection authority to offer Schrems II guidance is Germany's Baden-Württemberg Commissioner[3] which identified (i) Encryption, (ii) Anonymisation and (iii) Pseudonymisation as potential means for supplementing Standard Contractual Clauses (SCCs) to enable Schrems II lawful processing.

However, Max Schrems and NOYB (his privacy advocacy group)[4] take the position that Encryption does not satisfy Schrems II requirements.[5] In addition, only the most generalised non-relinkable Anonymisation can satisfy Schrems II.[6] This dramatically reduces the data utility for global processing, today and tomorrow. This leaves GDPR-compliant Pseudonymisation as the only means for adequately supplementing SCCs for lawful third-party cloud, SaaS and outsourcing arrangements.[7]

Anonos uses the term Data Liquidity→ to describe the ability to simultaneously achieve both universal data protection and unrivaled data utility. Anonos delivers Data Liquidity by leveraging GDPR-compliant Pseudonymisation together with patented state-of-the-art technology to transform data into a new secure data asset called a Variant Twin. With Variant Twins, it is virtually impossible for anyone other than an EU data exporter to re-identify data, because they provide protection for data while in use. **In addition, Variant Twins provide results with the same accuracy and value as when processing clear-text source data.**[8]



[1] See 16 July 2020 decision by the Court of Justice of the European Union in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18), "Schrems II") at https://www.anonos.com/judgment-of-the-court.

[2] All cloud, SaaS and outsource providers are impacted; the only exceptions are offerings by service providers organized under the laws of EU/EEA countries or countries having EU data privacy adequacy decisions and not making use of external cloud, SaaS or outsource capabilities from other countries. The only countries with valid EU adequacy decisions are Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay. See https://noyb.eu/en/next-steps-eu-companies-faqs.

[3] See English-language translation of German Guidance at https://privacytranslations.com/international_data_transfer

[4] NOYB initiated the Schrems II lawsuit that successfully invalidated the Privacy Shield and is suing over one hundred EU companies for failing to immediately comply with the Schrems II ruling which provided no grace period for compliance. See https://techcrunch.com/2020/08/18/eu-websites-use-of-google-analytics-and-facebook-connect-targeted-by-post-schrems-ii-privacy-complaints/

[5] NOYB challenges the notion that encryption can be an effective technical safeguard given the purported ability of the US government to break encryption. Encryption alone doesn't meet Schrems II challenges because encrypted,data is only protected at rest and in transit but has no utility, and when decrypted to provide utility in use, data is no longer protected. See https://noyb.eu/en/next-steps-eu-companies-faqs.

[6] NOYB highlights the US government's use of "selectors" to surveil EU personal data. These selectors may be "strong" (like email addresses, IP addresses or phone numbers) or "soft" (like indirect identifiers, keywords or attributes that by themselves do not identify a particular person, but when combined with other data can lead to re-identification). The use of "selectors" makes the use of anonymised data for Schrems II compliance impossible except for the most generalised, non-relinkable data. See https://noyb.eu/en/next-steps-eu-companies-faqs.

[7] See https://www.linkedin.com/pulse/does-gdpr-defined-pseudonymisation-overcome-encryption-magali-feys

[8] See https://www.anonos.com/variant-twin-value-proposition

Contact us at DataLiquidity@anonos.com for information on how Anonos Data Liquidity enables you to continue lawful international data transfers and secondary processing, including cloud, SaaS and outsourcing arrangements.