Prevent Schrems II Disruptions to Your Data Supply Chain

TOP 5 REQUIREMENTS

1 Immediately Implement Supplementary Measures for Lawful Transfer and Processing.[1]

a. The Schrems II ruling by the Court of Justice of the European Union in July 2020 did not require new standard contractual clauses (SCCs). Instead, it mandated the use of Supplementary Measures to ensure equivalent protection for all SCCs (old or new) to be lawful. *This obligation is immediate.*

b. In its final guidance, the EDPB clarified this means Technical Supplementary Measures that “must travel with the data wherever it goes” and identified GDPR Pseudonymisation for protecting data when in use. *Implementing Technical Supplementary Measures like GDPR Pseudonymisation is an immediate obligation for which there is no grace period.*

c. You have separate and independent obligations to transition to the new EU Commission SCCs by no later than December 2022. When you transition to the new SCCS, you must include a detailed description of Technical Supplementary Measures in Annex II.

d. Updating SCCs without new Technical Supplementary Measures is not enough.

2 Avoid Joint and Several Liability by Using GDPR Pseudonymisation.[2]

a. Under Clauses 3 and 12 of the new SCCs, data controllers and processors are jointly and severally liable to data subjects, each of whom can seek redress in EU courts.

b. Mandating the use of Schrems II compliant Technical Supplementary Measures like GDPR Pseudonymisation by all participants in data supply chains reduces liability and risk from improper processing by other parties with whom you process data and conduct business.

3 GDPR Pseudonymisation Uniquely Protects Data When in Use.[3]

a. If your business desires practical protection for data in use - not just when stored or transmitted - GDPR Pseudonymisation is the technical means to protect it. Learn more at Pseudonymisation.com.

b. In contrast, encryption does NOT protect data when in use and other data obscuring techniques like static tokenisation, key-coding and masking – which are sometimes incorrectly referred to as "pseudonymisation" are not up to GDPR standards; they do NOT protect data up to Schrems II standards when the data is in use.

c. GDPR Pseudonymisation is an underutilised tool for reconciling conflicts between maximising data value and enabling lawful use.

4 GDPR Pseudonymisation Enables Greater Lawful Data Use.[4]

It does so by helping to:

a. Support Lawful Data Repurposing, Sharing and Combining

b. Overcome Prohibitions Against Special Category Processing

c. Separate Processing Benefits from Re-Identification Obligations

d. Maximise the Availability of Lawful Profiling and Digital Marketing

e. Satisfy Data Protection by Design and by Default Obligations

f. Reduce the Risk of Data Breach Liability Obligations and Liability

g. Improve Scalability of Data Protection Impact Assessments

h. Enable Benefits of Expanded Lawful Processing

5 Localisation Does Not Make Schrems II Requirements Go Away.[5]

a. Suppose your organisation relies on advanced analytics, artificial intelligence (AI) or Machine Learning (ML). In that case, these critical processes cannot rely on Article 6(1)(a) or 6(1)(b) lawful bases of consent or contract when they cannot be adequately described at the time of data collection and are not essential for the performance of contract. Instead, you must have adequate technical and organisational controls in place – like GDPR Pseudonymisation – that protect data when in use to satisfy the balancing of interests test required for lawful Article 6(1)(f) legitimate interest processing.

b. You must satisfy GDPR Article 25 Data Protection by Design and by Default and Article 32 Security obligations, both of which explicitly highlight GDPR Pseudonymisation, even when data processing is localised in the EU.

c. When adequate technical controls are established as the default means of processing (e.g., to satisfy Schrems II, Legitimate Interests processing, Data Protection by Design and by Default, and Security requirements using GDPR Pseudonymisation), other processes requiring identifying personal data can be accomplished via (i) Article 49(1) derogations on an exception basis or (ii) localised processing.

Time is of the Essence for Avoiding Disruptions to Your Data Supply Chain

EDPB’s final Schrems II Guidance recommends “Adoption of strict data security and data privacy policies, based on EU certification or codes of conducts or on international standards (e.g. ISO norms) and best practices (e.g. ENISA) with due regard to the state of the art, in accordance with the risk of the categories of data processed.”[6]

Anonos Data Embassy is State-of-the-Art GDPR-compliant Pseudonymisation Software

Anonos is the only technology certified as satisfying the legal and technical requirements for GDPR compliant Pseudonymisation.[7]

EuroPrivacy.org
Privacy Audits and Certifications

Anonos “Best Practices” for Schrems II compliant transfers are included in the German Association for Data Protection and Data Security (GDD or Gesellschaft für Datenschutz und Datensicherheit e.V.) draft Code of Conduct for Pseudonymisation.

Anonos Data Embassy Software complies with all 50 of the GDPR-compliant Pseudonymisation Best Practices derived by Anonos from ENISA requirements specified at ENISAguidelines.com.

At the request of clients, Anonos developed the Data Embassy Quick Start program to provide the opportunity to start using Anonos GDPR-compliant Pseudonymisation software immediately to avoid disruptions to data supply chains. Data Embassy Quick Start software enables companies to reach an initial level of compliance within 48 hours of first contacting Anonos. Furthermore, by using Anonos Data Embassy software, organisations can reassure partners and customers that their organisation has taken the necessary initial steps to implement Schrems II compliant technical supplementary measures.

To learn more about Anonos Data Embassy software, go to:

Anonos.com/SchremsII-Solution

Anonos Data Embassy Software Does More Than Enable Schrems II GDPR Compliance

Implement Anonos Data Embassy software to achieve sustainable data value with utmost flexibility and customisability in using and sharing data globally.

No data… Little data… or all data… Gain complete control over how much information you share.

Tailor the level of identifiability for each use case, whether for analytics, AI or ML, data sharing, cross-border transfers, or future-proof other secondary data uses.

To learn more about Anonos Data Embassy software, go to:

Anonos.com/Sustainable-Data-Value

ENDNOTES

1. See Executive Summary and paragraphs 53 and 85 of the Final EDPB Guidance. See the Final EU Commission SCCs.
2. See the Final EU Commission SCCs.
3. See footnote 83 of the Final EDPB Guidance highlighting GDPR Article 4(5) requirements that GDPR-compliant Pseudonymisation consists of “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, **provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person,**” and adding that this additional information “may consist of tables juxtaposing pseudonyms with the identifying attributes they replace, cryptographic keys or other parameters for the transformation of attributes, or other data permitting the attribution of the pseudonymised data to identified or identifiable natural persons.” In contrast, encryption does not protect data when in use because it must be decrypted to enable use – see paragraphs 84 and 90 of the Final EDPB Guidance. The EDPB advises that encryption is not adequate for data transferred to US importers subject to FISA because of obligations to grant access to personal data in their possession, including cryptographic keys to render the data intelligible – see paragraphs 80 and 81 of the Final EDPB Guidance. See the video discussion on the Ten Truths of Pseudonymisation with the German Association for Data Protection and Data Security (GDD or Gesellschaft für Datenschutz und Datensicherheit e.V.) at www.SchremsII.com/TenTruths. Pseudonymisation is referenced 15 times in the GDPR compared to encryption which is referenced only 3 times and anonymisation which is referenced only 2 times in the GDPR.
4. See https://www.anonos.com/gdpr-pseudonymisation-benefits
5. See paragraph 83 of the Final EDPB Guidance.
6. See paragraph 141 of the Final EDPB Guidance.
7. See https://repository.europrivacy.org/en/certifications/edit/3ae8d3f2-d129-11e8-8e66-000c29bba468

Common Misconceptions
& Frequently Asked Questions (FAQs)

Anonos received 400+ requests for meetings following up on our Schrems II: Surviving and Thriving webinar, involving 3200+ from 2300+ companies and 50+ countries. Please read below to clarify the most common misconceptions and FAQs from our meetings to date.

1. **Does Schrems II Disrupt Data Supply Chains?**

   Yes, by eliminating parties from data supply chains that do not have adequate Technical Supplementary Measures. Suppose downstream data supply chain parties do not have adequate Technical Supplementary Measures like GDPR-compliant Pseudonymisation. In that case, upstream data providers will discontinue data flow rather than risk damaging their own business. Data is a precious resource for company performance and innovation, and without data flowing freely, critical opportunities for growth and revenue is lost. Therefore, Technical Supplementary Measures like GDPR-compliant Pseudonymisation are required to ensure ongoing data transfer and processing.

2. **Is there a grace period for complying with Schrems II requirements?**

   No. There is no grace period for complying with Schrems II – the obligation to comply was immediate upon the ruling of the CJEU on 16 July 2020.

3. **Can I Wait Until I Update My SCCs to adopt Technical Supplementary Measures?**

   No. The Schrems II ruling states that international data transfers using SCCs without adequate supplementary measures are unlawful. The ruling states in 5 places that the appropriate remedy for unlawful data transfers is immediate suspension or termination.

4. **Will EU-US Political Solutions Remove Requirements for Technical Supplementary Measures?**

   No. The philosophical differences between the US and EU approach to privacy are so fundamental that they will not remove requirements for Technical Supplementary Measures. US federal law and supreme court rulings favour a more commerce-friendly approach versus the EU view of privacy as a fundamental personal right that must be respected. If anything, Technical Supplementary Measures like GDPR Pseudonymisation may be required to achieve a new and sustainable treaty for lawful trans-Atlantic data flow.

5. **Can I Accomplish the Same Business Goals That I Did Before Schrems II When Using [insert name of cloud- or remote-based non-EEA software or service]?**

   Yes, but you may need to change how you use [insert name of cloud- or remote-based non-EEA software or service]. Advances in technology have made it seamless to transition from primary processing (the reason data is initially collected) to secondary (or further) processing like advanced analytics, artificial intelligence (AI) or Machine Learning (ML) using EU personal data. However, the lawful basis for primary processing under the GDPR rarely enables lawful secondary processing of the data for a different purpose. By leveraging GDPR-compliant Pseudonymisation and adopting new processes, you can achieve your business objectives while complying with your obligations under Article 6 - Lawfulness of Processing, Article - 25 Data Protection by Design and by Default and Article 26 – Security, as well as other GDPR obligations.

6. **Is Processing Pseudonymised Data as Accurate as Processing Data in the Clear (Cleartext Data)?**

   Yes. Unlike approaches like differential privacy and synthetic data which generally provide 20-30% or more distortion in results, properly implemented GDPR-compliant Pseudonymisation like that enabled by Anonos Data Embassy software retains 100% accuracy, fidelity, and value.

7. **If I Process Only Business-to-Business (B2B) Data, Do I Need to Comply with Schrems II.**

   Yes, if any of the data processed by you or by any of your B2B partners include any data that can be used directly or indirectly to identify a natural person, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.

8. **If I Do Not Process Personally Identifiable Information (PII), Do I Need to Comply with Schrems II.**

   Yes. EU personal data is not limited to direct identifiers. It also includes indirect identifiers, characteristics and other information that can be used directly or indirectly to identify a natural person, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.

9. **Are Schrems II Costs Just Another Compliance Expanse?**

   No. Anonos Data Embassy software embeds controls into your data, enabling it to lawfully flow across departments, divisions, companies, and borders to ensure compliance while simultaneously retaining 100% analytical accuracy and allowing 100% relinkability. This maximises data value and improves the scalability of operations while reducing the time to achieve insights, thereby turning the cost into an investment with a positive return.

10. **Can I use Encryption or Anonymisation as Supplementary Measures to Protect Data When in Use to Comply with Schrems II?**

    No. Encryption only protects data in transit and in storage. Anonymisation is not recognised as a suitable Schrems II Supplementary Measure. Schrems II requires organisations to protect data processed using SCCs by using Technical Supplementary Measures that "travel with the data wherever it goes" – including when in use – to ensure that EU personal data does not reveal the identities of data subjects when processed outside of the EEA / equivalency countries except as permitted by Article 49(1) derogations.