ANONOS

Schrems II[1] Misconceptions & Anonos Solution

In a world where most companies must rely on cloud computing and cross-border data transfers, the supreme court of Europe (CJEU) ruled in the landmark **Schrems II** case that "promises" to protect privacy in contracts and treaties are no longer enough.

To continue lawfully processing data in the cloud or outside of the EU, **companies must now prove they have technically-enforced privacy controls that protect data when in use -** encrypting data before and after use is no longer enough.

8 Misconceptions and FAQs

1 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.[2]

2 Can I just update Standard Contractual Clauses (SCCs) or wait for Privacy Shield II?

No. Words alone are not enough. SCCs "are not capable of binding the authorities of that third country, since they are not party to the contract."[3] No political solution to Schrems II will remove the obligation to implement new GDPR-compliant technical controls to reduce the risk of violating data subjects' fundamental rights for international data transfers to be lawful.

3 Must I stop all processing involving EU personal data that fails to comply with Schrems II?

Yes. Unless you implement technically-enforced Supplementary Measures, "you must avoid, suspend or terminate" all international data transfers based on SCCs.[4]

4 What is the penalty for failing to comply with Schrems II?

Under the CJEU ruling, Supervisory Authorities have an affirmative obligation to stop transfers that do not comply with Schrems II requirements.[5] In addition to business operation disruptions from termination of data flows, companies face penalties of **€20 million or 4% of their global turnover**, whichever is greater.[6]

5 Is Schrems II a C-Suite / Board level issue?

Yes. Due to the significant publicity regarding the potential negative effects of Schrems II, lack of corporate change may constitute "wilful blindness to a course of action" or "reckless conduct by knowing of the risk but doing nothing." This opens Board members and senior executives to potential personal and criminal liability.[7] In addition, auditors have an obligation to report data protection violations to authorities under the International Ethics Standards Board for Accountants (IESBA), and Non-compliance with Laws and Regulations (NOCLAR).[8]

6 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 by the European Data Protection Board (EDPB). Schrems II requires organisations to protect data when in use by using technically-enforced Supplementary Measures that protect data from unauthorised access. These technical controls must ensure that EU personal data does not reveal the identities of data subjects when processed outside of EEA / equivalency countries. **Processing of personal data in the clear outside of the EEA / equivalency countries is now unlawful.**[9]

7 Which processing can I no longer do?

Two use cases, which represent the majority or global data use and processing, are **now unlawful**:

- **Transfer to Cloud Services Providers or Other Processors Which Require Access to Data in the Clear** (EDPB Unlawful Use Case 6); and
- **Remote Access to Data for Business Purposes** (EDPB Unlawful Use Case 7).[10]

8 What are my options to comply?

New technical controls are required for the lawful transfer of **GDPR Pseudonymised data** (EDPB Lawful Use Case 2).[11] This means that Cloud Processing and Remote Access for Business Purposes (EDPB Unlawful Use Cases 6 and 7) can be *made lawful* by using GDPR-Pseudonymised data (Lawful Use Case 2).

Realize they MUST NOW HAVE a Technology-Enforced Defensible Business Position

* Participants in Anonos' Schrems II webinar on 29/10/2020 with 1800+ executives from 1700+ companies across 60+ countries.

Anonos
"crosses the chasm"
caused by:

TECHNOLOGY
Many technologists are not aware of Schrems II requirements

LEGAL
Many attorneys are not aware that technology exists that satisfies Schrems II requirements

SCHREMS II APPLIES TO YOU IF:

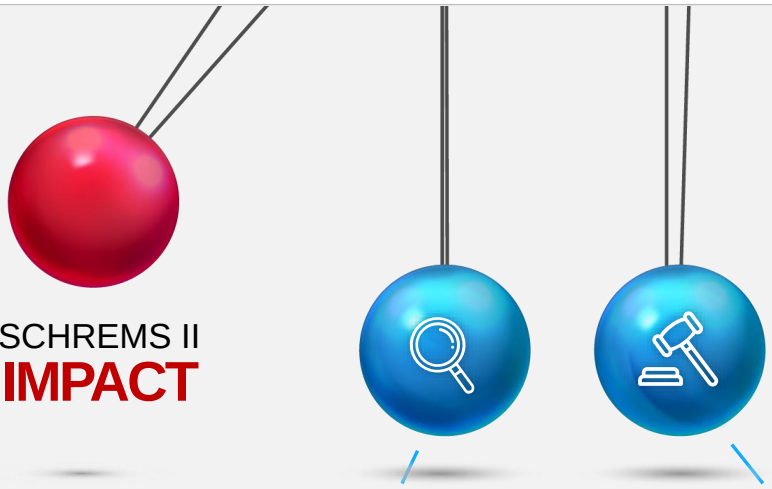
- Your company provides remote access to EU personal data for "follow the sun" support or analytics.
- Your company uses the "public cloud" to benefit from third-party analytics, AI or ML processing capabilities.
- You are a non-EEA / equivalency country advisory firm that processes EU personal data on behalf of clients.

Anonos Enables **Lawful Borderless Data**

Key Facts

- The Anonos solution is software that is securely installed and operated behind your firewall.
- Anonos does not have access to your data.
- Anonos software "functionally separates" information value from individual identities in data to enable you to satisfy the new heightened requirements for GDPR.
- Anonos software is the **only software that satisfies all 50 requirements** established by the European Cybersecurity Agency (ENISA) for GDPR-compliant Pseudonymisation.[12]

- Anonos was granted European Patent 3,063,691 in 2020 for **state-of-the-art technology**[13] **that achieves "the impossible" by balancing data protection and utility.**[14]
- Anonos ***guarantees*** that it **achieves the highest level of Schrems II and GDPR compliance while also enabling high data value and utility**.[15]



SCHREMS II
IMPACT

You must have technically-enforced Supplementary Measures to ensure that data "transferred" outside of EEA or equivalency **countries does not reveal identities of EU data subjects**

Processing EU data in the clear outside of the EEA or equivalency countries is now unlawful

When dealing with non-EEA / equivalency country vendors claiming that their services occur entirely within the EU, removing them from the realm of Schrems II issues, corporate officers and Boards of Directors are still open to risks. This is because while the data may appear to be accessed and processed solely only within the EU, **non-EU vendors often retain access to the data or to keys or other methods for accessing the data for purposes of performing services or other contractual obligations**.

IF YOU DO THIS[16]

Cloud-Based Processing of EU Data in the Clear

EXAMPLES

- **Banks** using analytics to study data on EU customers on “GCP”
- **Healthcare** companies using data sharing capabilities to query EU patient data on “AWS”
- **Media** companies using AI to process data about EU consumers on “Azure”

It is now Unlawful

Sharing EU Data for Business Purposes

EXAMPLES

- **Pharmaceutical** companies transferring EU clinical trial data to colleagues outside of the EEA for analysis
- **Global Advisory Firms** collecting data and processing results outside of the EEA
- **Insurance Firms** transferring EU data outside EEA for follow-the-sun Machine Learning (ML) capabilities

It is now Unlawful

98% of the participants in an Anonos Schrems II webinar held on 13 January, involving 2000+ executives representing 1700+ companies from 50+ countries, expressed concern about the risks associated with cloud-based processing of cleartext EU data and remote access to EU data for business purposes. In follow-up meetings and discussions with representatives from hundreds of companies, **grave concerns were raised by companies regarding the risk of personal and criminal liability for corporate officers and Boards of Directors for ongoing use of non-EEA Cloud, SaaS and outsourcing solutions.**

To mitigate these risks, companies should document the answers to the following questions in their files when vendors claim that their services occur entirely within the EU.

QUESTION
Does processing occur **solely** in the EU so that the Schrems II restrictions on international data transfers are not impacted?

01 Vendor Access In The Clear
When using a non-EEA/equivalency country vendor, is any data processed, or could be processed, in the memory of the vendor’s systems or otherwise so that **the data is accessible in the clear at any time by the vendor**, or through the vendor to authorities in any non-EEA/equivalency country, with respect to which the vendor is under an obligation to share, provide or disclose the data.

YES → **ANSWER: Risk of unlawful data use**

NO

02 Retained Keys
When using non-EEA/equivalency country software or services, **does the vendor retain any keys, copies of keys, or any other access mechanism** (e.g., “break the glass” access in emergency, non-payment or other situations) to provide the vendor with the ability to view or otherwise access your data in the clear at any time.

YES → **ANSWER: Risk of unlawful data use**

NO

03 Protected Indirect Identifiers
Does non-EEA/equivalency country software or services **protect not only direct identifiers but also indirect identifiers** so that in combination they do not reveal the identity of EU data subjects.

NO → **ANSWER: Risk of unlawful data use**

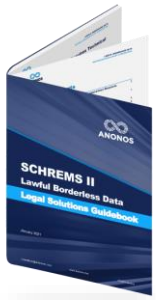
YES

ANSWER
Processing occurs **solely** in the EU so Schrems II restrictions should not present an Issue

SOLUTION
Unlawful data use can be made lawful with GDPR Pseudonymisation

ANONOS

Anonos delivers an **Immediate Defensible Position** to comply with Schrems II by providing:



1 Legal Guidebook with Templates

- **Appendix 1 highlights capabilities of Anonos Software -** *available only to licensed users* - **to help respond to inquiries from:**
  - Regulators (DPAs and vertical industry)
  - NGOs
  - Auditors (internal and external)
  - Stockholders
- **Appendix 4 guarantees for non-EEA / equivalency country vendors** to limit the potential liability of Board / C-Suite members
  - Mitigates risks when vendors claim that services occur entirely within the EU

2 Software Framework and Process

Software Framework and **Process** for delivering **"**Lawful Borderless Data**"**

- **Int'l Data Transfer Without Risk**
  - EDPB Lawful Use Case 2: Transfer of Pseudonymised Data
  - Compliance with ENISA requirements for Pseudonymisation
- **Data Utility without Compromise**
  - Patented Controlled Re-linkable Data
  - 2020 European Patent 3,063,691 for Dynamic De-Identification & Anonymity

3 Guaranteed State-of-the-Art Software

We guarantee that our software achieves the highest level of Schrems II and GDPR compliance while at the same time enabling the highest value and utility of EU personal data.[17]

Only Anonos delivers the following **benefits**:

- **Schrems II Compliant Supplementary Measures**
- **GDPR Compliant Pseudonymisation**
- **Future Proofed Standard Contractual Clauses (SCCs)**

Get in touch to establish an Immediate Defensible Position.
Reach us at LearnMore@SchremsII.com

See the following Schrems II resources:

Executive & Board Risk Assessment
Framework
VIEW

New Technology Controls Required
Framework
VIEW

IDC Report on Anonos
Embedding Privacy and Trust Into Data Analytics Through Pseudonymisation
VIEW

Executive Briefing Portal
60+ Videos with regulators and industry experts
VIEW

Linkedin Group
Over 4700 members
VIEW

Anonos Solution
Schrems II Compliant Supplementary Measures
VIEW

ENDNOTES

1. "Schrems II" refers to the ruling by the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, commonly referred to publicly as "Schrems II." Use of "Schrems II" in no way indicates any relationship or affiliation with, or endorsement by, Max Schrems or by the Non-Governmental Organisation, None of Your Business (NOYB), or any parties directly or indirectly associated with Max Schrems or NOYB.
2. See EDPB FAQs at https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf at page 2.
3. See http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404 at paragraph 125.
4. See EDPB Guidance at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf at page 3.
5. See http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404 at paragraphs 121, 135, 146, 154, and 203(3).
6. See GDPR Article 83(5)(c).
7. See https://normcyber.com/advisory-note/data-protection-directors-personal-liability/ and https://www.financierworldwide.com/roundtable-risks-facing-directors-officers-aug17
8. See https://www.ifac.org/system/files/publications/files/IESBA-NOCLAR-Fact-Sheet.pdf
9. See EDPB Guidance at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf
10. Ibid.
11. Supra, Note 9 at paragraphs 47, 48 and 80. The EDPB stresses that while "in principle, supplementary measures may have a contractual, technical or organisational nature...contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country...there will be situations where **only technical measures** might impede or render ineffective access by public authorities" (emphasis added).
12. Supra, Note 9 at paragraph 135. References to ENISA do not indicate any relationship, sponsorship, or endorsement by ENISA. All references to ENISA are intended to constitute nominative fair use under applicable trademark laws. See also https://www.ENISAguidelines.com.
13. See Recital 78 and Articles 25 and 32 for state-of-the-art requirements under the GDPR.
14. Anonos technology is protected by an international patent portfolio including Patent Nos. EU 3,063,691 (2020); US 10,572,684 (2020); CA 2,929,269 (2019) US 10,043,035 (2018); US 9,619,669 (2017); US 9,361,481 (2016); US 9,129,133 (2015); US 9,087,216 (2015); and US 9,087,215 (2015). See also https://www.Anonos.com/patents
15. Subject to contractual terms and conditions.
16. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by said companies.
17. Supra, Note 15.