ANONOS

Schrems II* Executive & Board
RISK ASSESSMENT FRAMEWORK

Hundreds of companies attended Anonos' Schrems II webinars, including regulators, industry experts, and leading non-governmental organisations (NGOs). This framework covers the crucial issues we address when working with these organisations to evaluate the ability to establish an immediately defensible position in compliance with Schrems II.

Schrems II: Impact on Operations

Two popular "mainstream" data processing activities were ruled illegal on 16th July 2020 by the Court of Justice of the European Union (CJEU). This case is known as "Schrems II", and the ruling is not appealable. The two data processing activities are:

- **Processing EU data "in the clear" by cloud service providers or other processors**
- **Providing non-EU companies access to EU data for business-related processing**

Encrypting data does not resolve this issue, and political solutions such as a new Safe Harbour / Privacy Shield Treaty have not materialized and are not likely to occur.

Two Main Risks to Business, Executives, and Boards

1. Risk of Business Disruption And Losses

The penalty for non-compliance with Schrems II is immediate termination of access to data, *not fines.*

a. Disruption to operations from terminated access to data can exceed any fine in its negative impact on business, revenue, and stock value.

b. The burden of proof for compliance is on an organisation in order to regain access and use their data.

2. Risk of Board / Executive Team Liability

Failure to take action to remedy Schrems II non-compliance over the 6+ months since the CJEU ruling can expose Boards of Directors / Executives to personal and criminal exposure.

a. "Wait and see" strategies increase the risk for potential claims of breach of fiduciary duties.

b. Potential options / actions should be evaluated and well documented in corporate resolutions and Data Protection Impact Assessments (DPIAs).

The hope for a political solution that resolves the issue does not mitigate these risks: **compliance and risk mitigation is required now using new technically-enforced controls.**

Guidelines for Risk Mitigation

The European Data Protection Board (EDPB) has published the following recommendations for complying with Schrems II:

a. The EDPB recommends transforming data into a new protected format called "GDPR Pseudonymisation".

b. The EU Cybersecurity Agency (ENISA) has established best practices for GDPR Pseudonymisation.

c. **ENISA-compliant GDPR Pseudonymisation technology is available now.**

d. Risk mitigation begins as soon as you engage with a technology provider as evidence of initial steps to comply.

* 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.

Frequently Asked Questions From Boards / Executives

1. **What is the Issue?** **Lost access to data.**
   The CJEU declared it illegal to (a) process EU personal data in US and other non-EU owned cloud infrastructure, and (b) outsource the processing of EU personal data to non-EU service providers. The Schrems II court decision is final and unappealable.

2. **Is there a Solution?** **Transforming data is recommended.**
   The EU regulators (EDPB) have recommended transforming EU personal data through GDPR Pseudonymisation before processing. GDPR Pseudonymisation does not degrade data accuracy or utility.

3. **What is the risk? Does insurance cover this?** **Risk of 100% penalty, likely no insurance coverage.**
   The remedy for non-compliance with Schrems II is the termination of data processing, which can equal a 100% penalty in the form of halted business operations. The Schrems II decision came out in July 2020, and there was no grace period for compliance. The passage of time could expose the company, senior management, and the Board to potential personal and criminal exposure. Many EU member states do not allow insurance coverage for General Data Protection Regulation (GDPR) breaches, such as the failure of organisations to comply with Schrems II requirements.

4. **What steps have we taken to address the situation?** **Wait and see is no longer an option.**
   Many companies, including ours, were hoping for political or legal solutions to the Schrems II situation. Recent opinions and investigations by EU legislators and regulators make it clear that a political solution is unlikely and new technical solutions are required because “legal only” solutions are insufficient. We are investigating vendors that can provide technically-enforced controls that meet EDPB requirements for GDPR Pseudonymisation.

5. **How long does it take to establish a defensible position?** **Within 24 hours.**
   One vendor that offers these technically enforced controls is Anonos. It provides a “Quick Start” solution that enables our company to establish an immediately defensible position. We can use a private-cloud hosted version of Anonos’ GDPR Pseudonymisation software to process industry and use case-specific sample data, providing proof of initial steps towards Schrems II compliance.

6. **What current operations need to be modified?** **Complementary to existing practices.**
   Anonos’ GDPR Pseudonymisation software complements our existing investments in cybersecurity and privacy technology. Anonos can work with our current lawyers and advisors or they offer partnerships with leading lawyers and advisors familiar with Anonos’ patented GDPR Pseudonymisation software.

7. **What parts of our organisation should be involved?** **Legal / privacy, data innovation, and technology.**
   Our legal/privacy team should confirm that Schrems II compliance requirements are satisfied. Our data innovation team should confirm that data innovation needs are met and data utility is maintained. Lastly, our technology team should confirm that existing investments in cybersecurity and privacy technology can be leveraged.

8. **How quickly can you provide an update?** **Within 24 hours.**
   Anonos is committed to providing us with an immediately defensible position by providing our company with access to a Quick Start implementation of their state-of-the-art GDPR-Pseudonymisation software within 24 hours of approval.

For more information on Anonos’ GDPR Pseudonymisation software, visit:

SchremsII.com/KnowledgeHub

LearnMore@anonos.com