Anonos releases guidance around the top 5 FAQs keeping businesses awake regarding Schrems II

BRUSSELS, BELGIUM, March 25, 2021 /EINPresswire.com/ -- Anonos, the leading provider of state-of-the-art data enablement and protection technology, today released guidance on the top 5 Frequently Asked Questions (FAQs) businesses are grappling with following the release of Schrems II preliminary guidance from the European Data Protection Board (EDPB).

Anonos - Lawful Borderless Data

Anonos releases guidance around the top 5 FAQ keeping businesses awake regarding Schrems II

In the guidance surrounding the future of lawful transatlantic data flows, the EDPB notes that "Transfer to cloud services providers or other processors which require access to data in the clear" (EDPB Use Case 5) are unlawful. However, the EDPB also notes that "Transfer of Pseudonymised Data" (EDPB Use Case 2) is lawful.

Below are the top 5 FAQs businesses engaging with Anonos are asking regarding the implications of EDPB Use Case 2 (Pseudonymisation) for transforming otherwise unlawful EDPB Use Case 5 (Cloud-based Processing), with guidance from Gary LaFever, CEO and General Counsel, Anonos, on the answers.

Q1: Does Pseudonymising EU data after it is in US-operated clouds or other technology platforms resolve Schrems II issues?

A1: No, Pseudonymisation must occur prior to transferring EU Personal Data to a US-operated cloud or other third-country-operated infrastructure. However, Supervisory Authorities may

hesitate to strictly enforce this requirement to provide companies the opportunity to remediate data already in the cloud by Pseudonymising it.

Subject to the possible one-time exception for remediation of data already in the cloud, EDPB Use Case 2 requires that the Pseudonymisation be performed by an EU data exporter prior to transferring the data to the cloud or other infrastructure. Adequate technical and organisational measures must be in place to ensure the non-relinkability of the EU data to identities without the use of "Additional Information" (sometimes referred to as "Keys"). These Keys must remain in the possession of the EU data exporter or a specifically enumerated authorised EU-based third-party, which clearly does not include US cloud or other third-country technology providers.

The above results are possible using advanced Pseudonymisation techniques that satisfy the requirements of GDPR Article 4(5) in accordance with best practices established by the European Cybersecurity Agency (ENISA).

Q2: How can my organisation comply with Schrems II requirements for data in US-operated clouds and other third-party technical infrastructures?

A2: Generally, there are 3 ways to comply with Schrems II requirements with respect to data in US-operated clouds and other third-party-operated infrastructures:

>First, cleartext EU personal data in US operated clouds and other third-party infrastructures can be replaced with properly Pseudonymised data. In the highest value use cases of Advanced Analytics, AI and ML, the results produced by lawfully processing GDPR-compliant Pseudonymised data have 100% accuracy and fidelity when compared to the results of processing in the clear. In addition to complying with Schrems II requirements, the processing of GDPR-compliant Pseudonymised data helps organisations comply with Secondary Processing obligations under Article 6.4 (for processing beyond purposes authorised by Consent or Contract), Data Protection by Design and by Default obligations under Article 25, and Security of Processing obligations under Article 32, which apply to all processing of EU personal data – whether internal or external to the EU.

>Second, when processing EU personal data in the clear is required, for example, to communicate with or with regard to an EU data subject, the desired use must fall within a GDPR Article 49 derogation.

>Third, if neither of the above two options are available, to comply with Schrems II requirements, the desired processing must occur within the EEA or a country that has received a valid EU equivalency decision (frequently referred to as "localisation").

Q3: How do cloud native business applications comply with Schrems II requirements?

A3: In contrast to cloud-based Advanced Analytics, AI and ML which can be successfully

supported using GDPR-compliant Pseudonymisation (see FAQ 2 above), cloud native business applications like O365, M365 and D365 must either (i) be supported by an Article 49 derogation or (ii) arrangements must be made for a non cloud-based solution to comply with Schrems II requirements.

GDPR Article 28(1) imposes an affirmative obligation on controllers to "use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of [the GDPR] and ensure the protection of the rights of the data subject." While US cloud and other third country infrastructure operators stress that they have valid Standard Contractual Clauses (SCCs) in place, SCCs by themselves do not make processing lawful under Schrems II. The Schrems II ruling holds emphatically that Supplementary Measures are required. However, cloud providers operate under a "Shared Responsibility Model", which makes it clear that responsibility for ensuring the lawfulness of application specific data is the obligation of the data controller. A careful reading of cloud provider data protection addendums verifies this result.

Q4: What is the penalty for Schrems II non-compliance?

A4: In the Schrems II ruling, the CJEU states five times that the GDPR-required remedy for violating Schrems II requirements is injunctive termination of processing since monetary damages cannot repurchase fundamental rights This highlights the immediate potential disruption to business operations and shifts the burden of proof onto data controllers to regain the right to process data. Since there is no grace period, compliance became mandatory as of the CJEU ruling in July 2020. Now, eight months later organisations must evaluate the availability of defences to overcome potential claims of non-compliance. Waiting to establish a defensible position for using US-based and other non-EEA cloud, SaaS, and outsourcing solutions creates the risk of personal exposure for Board members and officers. This risk is even more significant in the UK, where the UK GDPR includes additional provisions that impose criminal liability for non-compliance. In addition, auditors are starting to evaluate whether adequate balance sheet / claims reserves are set aside for future Schrems II related losses and are obligated to report non-compliance to authorities.

Q5: What is the Most Important Supplementary Measure for Schrems II compliance?

A5: The EDPB recognises three types of Supplementary Measures – Contractual, Organisational and Technical Supplementary Measures. However, the EDPB states that only one of the three types of supplementary measures is suitable for protection against foreign governments: technical measures.

The EDPB highlights GDPR-compliant Pseudonymisation as a Technical Supplementary Measure that "travels with the data."

Anonos is the source for GDPR-compliant Pseudonymisation that meets the state-of-the-art

requirements of the GDPR. For more information on Pseudonymisation visit: https://www.Pseudonymisation.com.

The EDPB highlights the importance of best practices established by the European Union Agency for Cybersecurity (ENISA). ENISA has released guidelines on requirements for GDPR-compliant Pseudonymisation. To view information on how Anonos meets all 50 of these requirements, visit: https://www.EnisaGuidelines.com/.

****
Schrems II Resources:

1) The Board Risk Assessment Framework is now available to view and download at https://www.SchremsII.com/Board2

2) Are you Schrems II Compliant Quiz (in 2 questions): https://www.anonos.com/TakeTheQuiz

3) Learn all about Pseudonymisation at https://www.pseudonymisation.com/

4) Schrems II Knowledge Hub: https://www.SchremsII.com/KnowledgeHub

5) Anonos: https://www.anonos.com/

Liberty Communications
on behalf of Anonos
email us here
Visit us on social media:
Twitter
LinkedIn
