New EU-US Trade and Technology Council Must Abide by Schrems II Requirements to be Lawful, Sustainable & ESG Compliant

WASHINGTON DC, USA, June 10, 2021 /EINPresswire.com/ -- Anonos, a leading provider of state-of-the-art data enablement and protection technology, has today commented on an upcoming EU-US technology and trade partnership in the context of the Court of Justice of the European Union (CJEU) "Schrems II" (1) ruling, the Standard Contractual Clauses (SCCs) announced on 4th June by the European Commission (EC) and the finalisation by the European Data Protection Board (EDPB) of Schrems II guidelines, expected on 18th June.

EU-US Trade and Technology Council (TTC) Must Abide by Schrems II Requirements

Schrems II Webinar: SCC & EDPB Requirements for Technical Measures

Obligations of New EU-US Partnership Under Schrems II

On 15th June, US President Joe Biden and EU Commission President Ursula von der Leyen are expected to announce a new EU-US Trade and Technology Council (TTC) partnership aimed at countering increasing Chinese dominance in the tech sector and promoting democratic values.

"From a data protection point of view, to satisfy Environmental, Social and Governance (ESG) considerations, the proposed TTC will need to abide by the CJEU's Schrems II ruling as well as follow-on actions by the EC and EDPB. Sustainable technology and trade decisions cannot be made without considering the ethical impacts on personal rights under the EU Charter of Fundamental Rights," said Magali Feys, founder of Belgian law firm AContrario and serving as

European Chief Ethical Data Strategist for Anonos.

“The Schrems II ruling requires organisations to cease the former practice of processing data ‘in the clear’ without protection in place during processing; this practice is unsustainable and exposes unprotected data to security and surveillance breaches. Protecting data during processing - not just when it is at rest or when it is in transit - makes data use sustainable plus increases privacy”, said Feys.

Benefits of GDPR Pseudonymisation for EU-US Data Flows and Partnership

“The Schrems II requirements for protecting data during processing do not go away because of an announced EU-US technology and trade partnership”, said Gary LaFever, CEO and General Counsel of Anonos. “Schrems II should be viewed as a positive by commercial organisations on both sides of the Atlantic as well as by government officials working on the new EU-US partnership.”

GDPR-compliant Pseudonymisation (2) serves as a technical safeguard recommended by both the EC (3) and the EDPB (4) that can protect data during processing as required under Schrems II but without degrading data value or quality, ironically enabling organisations to expand lawful data sharing and processing opportunities.

“GDPR-compliant Pseudonymisation can help to further the goals and objectives of the new EU-US Trade and Technology Council (TTC)”, said LaFever.

Implications of Schrems II Decision by Court of Justice of the European Union

Given the lack of judicial redress and the applicability of surveillance laws, the CJEU Schrems II ruling in July 2020 declared it unlawful to transfer EU data to the US (including processing of EU data in US operated clouds like Google, AWS and Microsoft Azure regardless of the location of equipment) without using new technology safeguards that protect the data during processing when there is a risk of surveillance.

As further context, it is important to note that:

+A joint initiative announced by the Presidents of the US and EU, representing the Executive Branches of each jurisdiction, does not alter the Schrems II ruling by the CJEU, an institution representing the separate and counter-balancing Judicial Branch of the EU government.

+Companies on both sides of the Atlantic are obligated to comply with Schrems II requirements - which have no grace period for enforceability - until the Judicial, Executive and Legislative branches of the EU and US governments reconcile fundamental conflicts between how the EU and the US view and enforce privacy rights.

+JUDICIAL CONFLICT: In the EU, the Schrems II ruling by the CJEU requires new technical safeguards to ensure EU-style data protection rights when data is processed in the US due to concerns over potential surveillance by government agencies. In contrast, the US Supreme Court recognises a “third-party doctrine” (5) under US law which holds that once a person voluntarily gives information to third parties like banks, phone companies, internet service providers, and email providers, they have "no reasonable expectation of privacy."

+EXECUTIVE & LEGISLATIVE CONFLICT: In the US, if an organisation tells a consumer what they plan to do with their data, they can do just about anything they want to so long as it was described to the consumer without violating privacy rights. In contrast, data protection is a constitutional right under the EU Charter of Fundamental Rights that cannot be infringed even if a data subject is made aware of an organisation’s intent to do so in advance.

Typically, data is technically protected only when at rest (in storage) or in transit (during transmission) by encrypting the data; when the data is processed, it is generally done ‘in the clear’ with no technical protection. Encrypted data must be decrypted to enable processing. At this point, it is unprotected and vulnerable to security breaches and potential surveillance by third party governments (including the US) revealing the identities of individuals. The Schrems II court held that technical safeguards must also protect the data when in use during processing when there is risk of surveillance - not just when at rest and in transit.

On 4th June, the EC published updated Standard Contractual Clauses (SCCs) which companies can use to transfer and process EU data in the US provided they comply with Schrems II requirements to put technical controls in place as required to prevent surveillance.

On June 18th, the European Data Protection Board (EDPB) is expected to adopt, at their next scheduled plenary session, the final version of their Schrems II compliance recommendations published in November 2020, further reinforcing the Schrems II requirements for protecting data during processing - not just when it is at rest or when it is in transit.

The EDPB recommends GDPR-compliant Pseudonymisation (6) (this is different from encryption and requires heightened security capabilities from what was required prior to the GDPR - see www.pseudonymisation.com) to protect data during processing.

While protecting data during processing using GDPR-compliant Pseudonymisation sometimes requires businesses to change how they process data, it increases opportunities to use, share and combine data improving ESG sustainability and resulting in a positive return on investment (ROI) for companies adopting GDPR-compliant Pseudonymisation.

Webinar on Surviving and Thriving Under Schrems II

The interrelationship of Schrems II requirements and the new EU-US Trade and Technology

Council (TTC) will be one of many topics addressed during a webinar Anonos is running on 22 June covering how to survive and thrive under Schrems II, for which over 2,000 people have registered. For more information on the webinar, visit www.SchremsII.com/Webinar.

For more information on how to continue lawful processing of EU data in compliance with Schrems II requirements using technical supplementary measures like GDPR-compliant Pseudonymisation, join the Schrems II Linkedin Group with nearly 8,000 members at: https://www.linkedin.com/groups/12470752.

FOOTNOTES:

(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."

(2) GDPR Article 4(5) requires 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." See also the video discussion on the Ten Truths of Pseudonymisation with Steffen Weiss from the German Association for Data Protection and Data Security (GDD or Gesellschaft für Datenschutz und Datensicherheit e.V.) at www.SchremsII.com/TenTruths.

(3) See Section 8.5 of ANNEX to the COMMISSION IMPLEMENTING DECISION (https://ec.europa.eu/info/sites/default/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf) for MODULE ONE: Transfer controller to controller, and Section 8.6 of MODULE TWO: Transfer controller to processor, MODULE THREE: Transfer processor to processor, and MODULE FOUR: Transfer processor to controller.

(4) See Paragraph 80 of EDPB Recommendations 01/2020 (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf).

(5) US Supreme Court decisions in United States v. Miller, 425 U.S. 435 (1976) and Smith v. Maryland, 442 U.S. 735 (1979) hold that individuals do not have a reasonable expectation of privacy in checks and deposit slips they give to banks (Miller) and phone numbers they dial (Smith) since in exposing them to third parties they assume the risk the information could be handed over to the government.

(6) Supra, Note 4.

Liberty Communications

on behalf of Anonos
email us here
