Statutory Pseudonymisation is Key Under GDPR and Global and US State Privacy Laws

Trans-Atlantic Data Transfers Under Proposed EU-US Arrangement Should Embrace EU Recommended Technical Supplementary Measure to Avoid Invalidation Like Schrems

EU-US Pact Should Embrace Statutory Pseudonymisation as a Technical Supplementary Measure

BRUSSELS, BELGIUM, March 29, 2022 /EINPresswire.com/ -- Last week US President Joe Biden and EU Commission President Ursula von der Leyen jointly announced that the US and EU have reached "an agreement in principle on a new framework for transatlantic data flows" to "enable predictable, trustworthy data flows between the EU and the US, safeguarding privacy and civil liberties."

"However, a review of the situation from the following perspectives highlights the narrow path required for any such arrangement to be sustainable, "said Gary LaFever, CEO and General Counsel of Anonos. "Any hope of a sustainable resolution of the desire for strong trans-Atlantic data flows in compliance with both EU data protection laws, and US surveillance laws should include scrutiny of the requirements for and the statutory benefits of Pseudonymisation as a compliant technical supplemental measure under the CJEU Schrems II decision."

National Security Pressures: Earlier the same week as the joint press conference, Politico reported in The Supreme Court just made a US-EU Privacy Shield agreement even harder that "The U.S. Supreme Court's decision this month in FBI v. Fazaga, a case challenging FBI surveillance, will make it significantly harder for people to pursue surveillance cases, and for U.S. and European Union (EU) negotiators to secure a lasting agreement for transatlantic transfers of private data...The justices gave the U.S. government more latitude to invoke "state secrets" in spying cases. But ironically, that victory undercuts the Biden administration's efforts to show that the United States has sufficiently strong privacy protections to sustain a new Privacy Shield agreement — unless Congress steps in now." It is critical to note that the reason for the invalidation of the prior Privacy Shield treaty enabling lawful trans-Atlantic data flows by the

supreme court of the EU - the Court of Justice of the European Union (CJEU) - was concern over the surveillance of EU citizens by US government agencies.

Executive Order versus Congressional Action: It is important to note that only a "deal in principle" has been reached, indicating an understanding that could lead to an actual "deal." All indications are that such a deal would be in the form of an Executive Order enabling President Biden to act without requiring Congressional endorsement. However, executive orders are only temporary until a new President decides to undo them. The CJEU ruling in the Schrems II decision (the case brought by privacy advocate Max Schrems that led to the invalidation of the Privacy Shield) requires either:

- Guarantees in law which can only be achieved by an Act of Congress (the current Congress is too bipartisan currently to pass a law limiting the scope of US surveillance); or

- Technical supplemental measures recommended by the EDPB and by the EDPS that enable ongoing data processing while safeguarding the fundamental rights of EU citizens to privacy and data protection under the EU Charter of Fundamental Rights.

Obligations of EU Member State Data Protection Authorities (DPAs): Even if the EU Commission were to pass a treaty, based on an Executive Order issued by President Biden, DPAs from all 27 EU member states would be legally obligated under the CJEU Schrems II decision to force companies to suspend transfers if there is not an essentially equivalent level of protection in the US as there is in the EU.

Attention of Advocacy Groups: As reported by TechCrunch, "Max Schrems, the privacy lawyer and campaigner whose name has become synonymous with striking down transatlantic data transfer deals (aka, Schrems I and Schrems II) was quick to sound a note of scepticism over what's been cooked up this time. So, his assessment of the text, when it emerges, will arguably have rather more weight than the Commission's. Via his privacy advocacy not-for-profit, noyb, Scherms also said he expects to be able to get any new agreement that does not meet the requirements of EU law back to the CJEU within a matter of months (e.g. via civil litigation and preliminary injunction)."

GDPR-compliant pseudonymisation helps to enable lawful international transfer and processing of global data by establishing by default the processing of protected GDPR-compliant pseudonymised data whenever, wherever, and as often as possible (as required by GDPR Articles 25 and 32) to ensure protected processing within the control of the EU Data Controller (a Data Embassy, as it were) so that non-pseudonymised (i.e., identifying) data is processed only when authorised and necessary to satisfy GDPR Articles 5(1)(b) Purpose Limitation and 5(1)(c) Data Minimisation requirements.

The challenge is that most people are not up to speed on what is required to satisfy the requirements and reap the statutory benefits of Pseudonymisation - both under the GDPR as

well as an increasing number of US state privacy laws (e.g., the California, Virginia and Colorado privacy laws which have adopted the GDPR definition of the term).

The lack of clarity regarding the requirements for and benefits of statutory Pseudonymisation was the topic of a January webinar (https://www.linkedin.com/pulse/2022-year-gdpr-pseudonymisation-gary-lafever/) on this topic as well as the inaugural February Pseudonymisation Podcast (https://www.anonos.com/announcing-the-launch-of-the-pseudonymisation-podcast), sponsored by a LinkedIn group of over 9,400 senior global privacy professionals advocating for increased awareness of statutory Pseudonymisation (https://www.linkedin.com/groups/12470752/).

About Anonos

Data is the world's most precious resource, and its value is often truly realised only when it's shared and combined with other data. Anonos empowers organisations with more opportunities for sustainable applications by protecting it at rest, in transit, and in use, both now and in the future. Anonos recognises that protecting data privacy is about much more than compliance: the Anonos team has invested over nine years and tens of thousands of hours into solutions that future-proof global data use and compliance. The only software to utilise GDPR-compliant Pseudonymisation and patented relinking techniques, Anonos Variant Twins make it possible to legally analyse, combine, and use data both inside and outside of organisations.

PR
Anonos
email us here
Visit us on social media:
Twitter
LinkedIn
