SCHREMS II WEBINAR: END TO REGULATORY ARBITRAGE

All-Star Webinar Panel Highlights the Need for Additional Measures for International Data Transfer

BRUSSELS, BELGIUM, October 14, 2020 /EINPresswire.com/ -- Anonos announced today the availability of a summary, video replay, transcript, and FAQs from last week's all-star Schrems II panel. The panel included representatives from the European Data Protection Supervisor (EDPS), Max Schrems' privacy advocacy group, None of Your Business (NOYB), and industry experts Promontory, fieldfisher, Cooley and Anonos at SchremsII.com/summary.

The timeliness and importance of the subject matter of the Schrems II - Lawful Data Transfer webinar was evidenced by the fact that more than 2,300 people registered for the event in under 72 hours, greater than half of whom watched the event live. During the webinar, over 900 questions were asked, and within 24 hours of the webinar, over 1,000 people had joined the new Schrems II Lawful Transfer Linkedin Community Group.

The Schrems II decision by the Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield for

Schrems II Lawful Data Transfers with NOYB, EDPS and Industry Experts - SUMMARY

Schrems II Webinar - Lawful Data Transfer (Presented by Anonos)

international data transfers involving EU personal data, effectively imposing “precision” on general obligations under the GDPR. The court ruling prescribes that EU data can no longer be lawfully processed in US-operated (or any other non-EU operated) clouds, SaaS or outsourcing services without “additional safeguards” that prevent the data from being subject to surveillance by the US (or other non-EU countries).

The webinar panelists discussed these “additional safeguards” now required for lawful cloud processing, SaaS and outsourcing.

One issue that all of panelists unanimously agreed upon, as did 94% of the webinar attendants, was that a two-step privacy-respectful Data Protection by Design and by Default approach is required for all processing whenever possible. This includes, but is not limited to, international data transfers following the CJEU decision in Schrems II.

Previously, some companies engaged in “regulatory arbitrage” by choosing not to comply with privacy laws, and baking the cost of non-compliance into the cost of doing business. Of great significance is the fact that the CJEU ruled that such unlawful data transfers and processing must be stopped, rather than fined. This makes a “regulatory arbitrage” approach impracticable – lack of access to data halts business operations, and cannot be merely calculated into the cost of doing business.

Anna Buchta, Head of Policy & Consultation at the EDPS, explained during the webinar:

“From the point of view of the regulators, we at EDPS and others have said many times already given the fundamental constitutional importance of this ruling, there has to be a before and after Schrems II. There will have to be consequences and that, unfortunately, may mean that certain transfers will not be able to continue with the available legal instruments without “additional safeguards” to ensure equivalent protection as under the GDPR... as I said, we need to realize that Schrems II has to have an actual impact in practice and I'm sure that this is also in this direction that the forthcoming guidance from the European regulators will go.”

Senior NOYB lawyer, Romain Robert, elaborated further that many of the current “additional safeguards” that are being considered, should in fact already be in place before any transfers take place. He noted that::

“Security measures and encryption should already be there before any transfer because it's an obligation under the GDPR and Article 32 so it’s an obligation for security. Pseudonymisation as well is also mentioned a lot of times in the GDPR but before any transfers. Pseudonymisation is not the solution to transfers. It should be done before any transfer in a specific situation like if you want to justify, for example, the change of purpose or if you want to evaluate the risk on the DPIAs.”

Mark Webber, Managing Partner at the Silicon Valley office of the law firm fieldisher, noted the

importance of employing additional measures to protect data, but raised a potential concern about the potential ramifications of Schrems II for limiting technological innovation:

“I, for one, am very serious about privacy, but I don't want to see this lead to more localisation, less use of the internet, and less use of technologies which will change our worlds. I think the majority of people on this conference call have survived in COVID because of their ability to turn to the internet, and the internet is a great game changer for all, and I think we've all got a role in making sure we can continue to use those technologies and work with those businesses too for the good of everybody. I think being creative and working together to do that is where I think it has helped.”

With the COVID pandemic, many companies are relying even more heavily on cloud and SaaS services for timely insights about partner and customer ecosystems. However, the Schrems II decision makes many cloud and SaaS services involving international data transfer unlawful without new additional technical safeguards.

A recent IDC Vendor Profile titled Embedding Privacy and Trust Into Data Analytics Through Pseudonymisation (IDC #EUR146734820) highlights the following about technology from Anonos, the host of the Schrems II webinar:

Anonos’ BigPrivacy software is well placed to satisfy the Schrems II requirements for appropriate safeguards by creating pseudonymised versions of personal data (Variant Twins). Variant Twins ensure that desired processing results are achievable without providing third parties, including country authorities, the ability to re-identify individuals.

About Anonos:

Anonos patented “Data Liquidity” technology simultaneously achieves Universal Data Protection and Unrivaled Data Utility by embedding controls that flow with the data to enforce protection at the time of use. Anonos enables the maximum lawful liquidity value of data for sharing between parties to support AI, ML, and BI applications and many others. With Anonos, companies can leverage their internal and external data while guaranteeing individual privacy rights as required under evolving data protection laws. Anonos has achieved what many thought was impossible: technology enabling data to be used and shared with the accuracy of clear text in a non-identifying and lawful manner. See https://www.anonos.com

MEDIA CONTACT
Liberty Communications on behalf of Anonos
+44 20 7751 4444
email us here
Visit us on social media:
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/528339533

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2020 IPD Group, Inc. All Right Reserved.