How to Answer Data Protection Authority Questions on Schrems II Compliant Supplementary Measures

German DPAs have starting sending out questionnaires regarding the lawfulness of data transfers under Schrems II.
In Question 9 from **their Intragroup data transfer** questionnaire they ask:

Q9. What supplementary measures have you implemented if your data importer cannot guarantee that there is no risk of surveillance?

Of Three Types of Supplementary Measures, only ONE works if surveillance is possible:

1. ~~Contractual Supplementary Measures~~

2. ~~Organisational Supplementary Measures~~

"...if the data importer or any further recipient to which the data importer may disclose the data falls under 702 FISA49, SCCs or other Article 46 GDPR transfer tools may only be relied upon for such transfer if additional supplementary technical measures make access to the data transferred impossible or ineffective." See pg. 15 of EDPB Recommendations 01/2020 on Supplementary Measures

3. **Technical Supplementary Measures** ✓

Technical Supplementary Measures are required See para 48 of EDPB Recommendations 01/2020

Implementing Technical Supplementary Measures

EDPB identified five technical controls as valid Technical Supplementary Measures:

I. Encryption of data at rest
II. **GDPR Pseudonymisation*** ✓
III. Encryption of data in transit
IV. Protected Recipient
V. Split Processing

Of the five Technical Controls noted by EDPB, only "GDPR Pseudonymisation" transforms Illegal Cloud Processing and Remote Access into lawful processing by Pseudonymising data before leaving the EU.

*See German Association of Data Protection and Data Security (GDD) and Anonos Ten Truths of GDPR Pseudonymisation at SchremsII.com/TenTruths

ANONOS DATA EMBASSY TECHNOLOGY ENFORCES GDPR PSEUDONYMISATION

DATA EMBASSY TECHNOLOGY TRANSFORMS UNLAWFUL SECONDARY PROCESSING INTO LAWFUL SECONDARY PROCESSING

UNLAWFUL SECONDARY PROCESSING	ANONOS	LAWFUL SECONDARY PROCESSING ✓
CLOUD PROCESSING OF EU DATA IN THE CLEAR REMOTE ACCESS TO EU DATA IN THE CLEAR	→	GDPR PSEUDONYMISATION = LAWFUL BORDERLESS DATA WITH 100% ACCURACY

ANONOS DATA EMBASSY TECHNOLOGY

Embedded technical controls that travel with the data to enable Schrems II compliant:

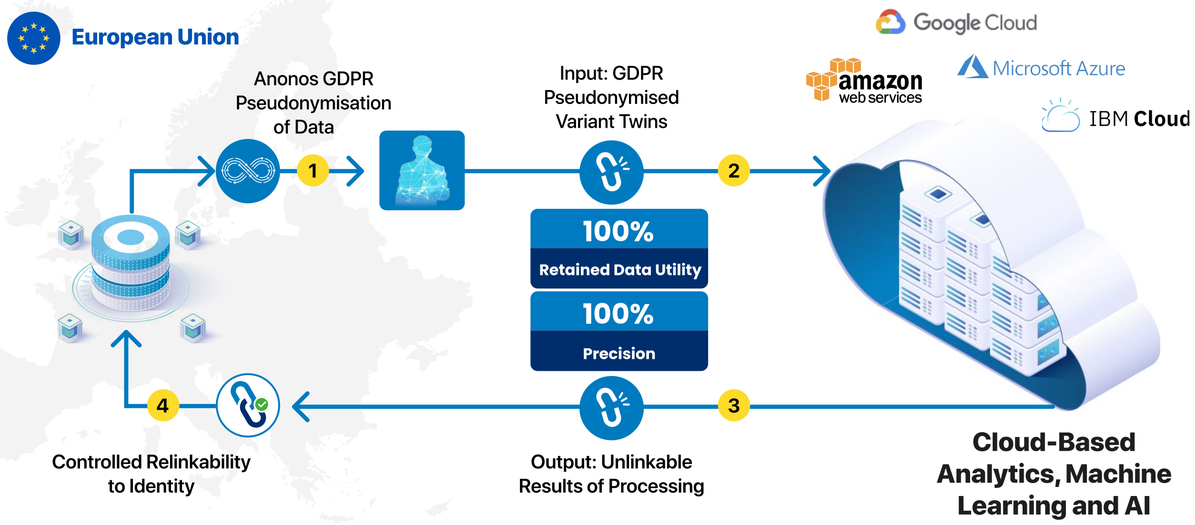
- Cloud and remote-based secondary processing for analytics, AI & ML
- Cross border transfers
- 100% accuracy
- Relinkability to identity only by data controller in the EU
- Data sharing & combining

In contrast to data localisation, Anonos Data Embassy technology enables one country's data to be transferred to and processed in a second country in compliance with the laws of the first country via embedded technical controls.

Presented by ANONOS | LearnMore@anonos.com

Anonos Lawful Borderless Data = Maximum Data Protection and Value Maximisation

ANONOS DATA EMBASSY TECHNOLOGY TRANSFORMS UNLAWFUL TO LAWFUL SECONDARY PROCESSING



EXAMPLE: ANALYTICS, AI & ML

1. EU data controller uses Anonos Data Embassy technology to Pseudonymise data in the EU.
2. Pseudonymised data is input for public cloud processing.
3. Pseudonymised results with 100% accuracy are the output.
4. EU data controller relinks results to identifying data in the EU.

Edge cases not covered by Anonos Data Embassy technology include applications like email and customer communications requiring precise data subject identities which must be supported via Article 49(1) derogations or localisation of processing within the EEA / Adequacy Countries. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of these marks does not imply any affiliation with or endorsement by these companies.

The only software to utilise GDPR-compliant Pseudonymisation together with patented relinking techniques, Anonos Variant Twins make it possible to analyse, combine, and use data both inside and outside organisations, in a variety of different use cases. With the ability to obscure key identifiers—but not permanently alter or remove them—Anonos Data Embassy technology protects data subjects without depriving organisations of the key insights that can only come from clear, accurate data. Variant Twins embed mandated protections into data, allowing it to reach its infinite, legal potential.

Data is an organisation's most precious resource. While data is useful internally, its value is only truly realised when it can be shared and combined with other data sets. However, as the value of data has grown, the risk and complexity of leveraging it has grown even faster. Organisations pour resources into deriving more value from data while critical investments in protecting data subjects lag behind, even as data privacy regulations proliferate and the punishments grow more severe. Control over data is increasingly equated with localisation or keeping it in-house—a decision that stifles innovation, obstructs growth, and erodes the very value of the data itself.

Creating sustainable value from data requires lawful control custom for each use case.

Anonos Variant Twins enable functional separation by embedding technical enforcement of policies into the data to enable maximum flexibility: *now organisations can share no data, a little data, or a lot of data in any volume, or level of identifiability* as required to support lawful analytics, AI & ML, internal data sharing, external data sharing, and cross border transfers and future-proofed other secondary data uses.

When using Variant Twins, organisations do not have to include all source data about a data subject in protected output to get back to and augment all of the source data about the individual. Information about data subjects can be included in multiple Variant Twins, each associated with a different group representing a sufficiently small number of people to accurately reflect details regarding shared behaviours, characteristics, interests, etc. Still, large enough so that no identity is revealed by ensuring the risk of unauthorised re-identification satisfies a minimum established level.

Information associated with group-level Variant Twins in which an individual belongs can be used to augment the source data for the individual with "Provided Data" (information provided by the members of the group or by third parties with the permission of group members), "Observed Data" (information captured by recording the actions of the group members) and "Inferred Data" (information created or derived through the analysis or interpretation of data) for the group. In this way, Variant Twins deliver 100% of the precision and results available when processing unprotected data in the clear but with maximum data protection and utility.

You Have Two Options to Choose From:

Business Continuity Risk from "Breaks" in Your Data Supply Chain

Technical supplementary measures are required to comply with Schrems II when there are risks of surveillance - ***including secondary processing in US-operated clouds and via remote access.***

You face **risks of termination of access to critical data supply chains** by partners unwilling to take the risk of negative impacts to their operations from halted processing by supervisory authorities

OR

Uninterrupted Data Flows With an Immediately Defensible Position

Anonos Data Embassy technology transforms personal data into privacy-respectful GDPR-compliant Pseudonymised data that embeds controls that travel with the data to enforce policies for Schrems II compliance.

Anonos Quick Start Data Embassy program provides an **Immediately Defensible Position** as proof that your organisation has started the process to use state-of-the-art technology to comply with Schrems II requirements for lawful cloud and remote secondary processing for analytics, AI & ML.