Memorandum

To: European Data Protection Board
From: Magali Feys (magali.feys@anonos.com)[1]
Gary LaFever (gary@anonos.com)[2]
Date: 29 July 2020
Subject: Supplemental Measures Under Schrems II

The European Data Protection Board ("EDPB"), in their Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems,[3] stated that:[4]

> *"The EDPB is currently analysing the Court's judgment to determine the kind of supplementary measures that could be provided in addition to SCCs or BCRs, whether legal, technical or organisational measures, to transfer data to third countries where SCCs or BCRs will not provide the sufficient level of guarantees on their own.*
>
> *The EDPB is looking further into what these supplementary measures could consist of and will provide more guidance."*

As a complement to longer-term development of a political resolution to the international challenges underlying the invalidation of the EU-U.S. Privacy Shield under Schrems II,[5] **this Memorandum proposes using "Data Embassy Principles" (as described herein) to enforce EU data protection obligations.**

Executive Summary

The COVID pandemic is accelerating the need for data-driven innovation and digital transformation. However, the Schrems II case ruling by the Court of Justice of the European Union ("CJEU") has turned the world of international data transfers upside-down. **Overnight, thousands of organisations are now looking to the EDPB for timely guidance.**

The court in Schrems II made the far-reaching decision to invalidate the EU-US Privacy Shield, and to require that many Standard Contractual Clauses ("SCCs") must include "supplementary measures" to

1 Magali Feys is Chief Strategist of Ethical Data Use at Anonos and founder of AContrario Law, a boutique law firm specialising in IP, IT, Data Protection and Cybersecurity. In addition, Magali acts as a legal advisor of the Belgian Ministry of Health where she advises on privacy related matters and is a member of the legal working party e-Health of the Belgian Minister for Public Healthcare.

2 Gary LaFever is Co-Founder, Chief Executive Officer and General Counsel at Anonos, a former partner at the international law firm of Hogan Lovells and former Management Information Consultant at Accenture. Gary's 35+ years of technical and legal expertise enables him to approach data protection and utility issues from both perspectives. He is a co-inventor of 17 granted patents with over 70 additional patents pending in the U.S. and internationally.

3 See Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems at https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf ("EDPB FAQs")

4 See FAQ 10 of the EDPB FAQs

5 *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18), "Schrems II"). See http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404

ensure that data subjects' rights are protected at the same level as they would be within the EU: essentially, compliant with the GDPR.

As yet, no official guidance has been released on what "supplementary measures" could be used to meet the requirements in Schrems II. **It is our proposal that a Functional Separation approach, enabled through GDPR-defined Pseudonymisation and the use of the resulting secured Personal Data, could serve as a model supplementary measure in this context.**

We further describe this below, in our enumeration of what we call "Data Embassy Principles," which embed risk-based controls into data. This allows risk to be managed wherever data goes, even during data sharing, combining, or transforming. This approach uniquely helps to satisfy global requirements for compliant innovative data use, including the new requirements set out by Schrems II. We believe these principles could be helpful for the EDPB in their search for appropriate "supplementary measures" and "appropriate safeguards" in light of Schrems II.

Proposed "Appropriate Safeguards" to Meet Schrems II Requirements

In Schrems II,[6] the CJEU highlighted the requirement in GDPR Recital 108 that:

> *"…in the absence of an adequacy decision, the **appropriate safeguards** to be taken by the controller or processor in accordance with Article 46(1) of the regulation must 'compensate for the lack of data protection in a third country' in order to 'ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union."*[7] (emphasis added)

The importance of providing appropriate safeguards is highlighted over twenty times in Schrems II.[8] However, legal experts note that Schrems II does not provide guidance on what "appropriate safeguards," "additional safeguards," "supplementary measures," or "effective mechanisms" mean, despite the fact that they play a central role in the court's decision.[9]

The Data Embassy Principles described in this Memorandum, are drawn directly from the GDPR itself. However, they are organised in a manner that helps make clear how they satisfy Schrems II requirements for "supplementary measures" now required for SCCs and Binding Corporate Resolutions ("BCRs"). **Data Embassy Principles help to supplement SCCs and BCRs at a time when international data transfers are urgently needed to alleviate the ravages of COVID-19 and to ensure economic viability around the globe.**

For any "supplementary measures" under Schrems II to be effective, they must balance privacy rights *and* data utility, or they negate the purpose of the global data sharing: to use the data. Measures that protect privacy and data to an extremely high level, but remove data accuracy and utility, are not effective in the

6 Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Case C-311/18), "Schrems II"). See http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404

7 *Supra,* Note 2. at paragraph 95.

8 For example, see *Supra,* Note 1, at Reference for preliminary ruling and paragraphs 8, 14, 15, 19, 91, 92, 95, 103, 105, 128, 131, 202, and 203.

9 For example, see https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

environment of international data flows. The same limitations exist for measures that provide protection at rest and in transit, but fail to provide protection while data is in use.

Data Embassy Principles are also consistent with recommendations by the forerunner of the EDPB, the Article 29 Working Party ("WP29"), and the European Data Protection Supervisor ("EDPS") for the use of "Functional Separation." Functional Separation involves separating information value from identity to enable the discovery of trends and correlations independent from any subsequent authorised application of the insights gained to the individuals concerned. By enforcing Functional Separation as described in the Data Embassy Principles, organisations may be able to continue:

- Transfers of EU personal data in compliance with the decision in Schrems II; and
- Processing protected data in other countries in accordance with local requirements.

In *Opinion 03/2013 on Purpose Limitation,* the WP29 highlighted the "prominent role in our analysis for different kinds of safeguards, including technical and organisational measures to ensure **functional separation**, such as full or partial anonymisation, pseudonymisation, aggregation of data, and privacy-enhancing technologies."[10] In addition, a 2015 report by the EDPS, *Meeting The Challenges of Big Data – A Call For Transparency, User Control, Data Protection By Design And Accountability*, highlighted **functional separation** as a potential solution to help resolve conflicts between innovative data use and data protection.[11]

Under the GDPR, the concept of Functional Separation is embodied in Article 4(5) and the definition of "Pseudonymisation". This definition requires that the information value of data must be separated from the identity of data subjects and that additional securely-stored information must be necessary to re-identify data subjects, and then only under controlled conditions.[12] *It is critical to note that under the GDPR, Pseudonymisation is now defined as an outcome and not a technique*. Our experience is that the existence, and more importantly the significance of this change, is not well appreciated outside the EU regulatory community. Over time we anticipate that the foresight in making this fundamental change will become clear due to its broad utility and effectiveness in resolving conflicts between innovative data use and data protection.

Before the GDPR, Pseudonymisation was widely understood to mean replacing direct identifiers with tokens, and was applied to individual fields independently within a data set. It was merely a Privacy Enhancing Technique ("PET").

With the elevation of Pseudonymisation now to an outcome, to achieve GDPR-compliant Pseudonymisation it has become necessary to protect not only direct identifiers but also indirect identifiers. In addition, instead of being applied only to individual fields, GDPR-defined Pseudonymisation, in combination with the GDPR definition for Personal Data, now requires that the outcome must apply to a data set as a whole (the entire collection of direct identifiers, indirect identifiers and other attributes), and

10 See https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf at pages 13, 26, 27, 29, 30, 31, 32, 33, 40, and 46.

11 See https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf at page 15. Additional information on functional separation is available at www.MosaicEffect.com

12 The principle of functional separation also exists under other data protection laws using different terms – e.g. heightened "De-Identification" under the California Consumer Privacy Act (CCPA) and the proposed Indian Data Privacy Law, and "Anonymisation" under the Brazilian Data Protection Law.

consideration must be given to the degree of protection applied to all attributes in a data set. Finally, the foregoing must be accomplished while still preserving the data's utility for its intended use.

As a result, pre-GDPR approaches (using a static token on a direct identifier, which unfortunately is still widely and incorrectly referred to as "pseudonymisation") will rarely, if ever, meet the heightened GDPR requirements of Pseudonymisation.[13] **This also means that old approaches known as "pseudonymisation" will not be sufficient to meet the requirements** for supplementary measures to enable lawful international data transfers under EU law.

GDPR Recitals 78, 85, and 156 and Articles 6(4)(e), 25, 32, 40, 89 specifically recognise properly Pseudonymised data – *as per the new standards as now defined under the GDPR* – as an appropriate safeguard to help satisfy GDPR requirements. The term "Pseudonymisation" is used fifteen (15) times in the GDPR, compared to "Encryption" which is used only four (4) times, and "Anonymisation" which is used three (3) times. No other Privacy Enhancing Technique (PET)[14] is referenced in the GDPR. Accordingly, the GDPR expressly awards benefits to the use of GDPR-compliant Pseudonymisation including, but not limited to, the following:

- Tipping the balance in favour of Legitimate Interests processing (Articles 5(1)(a), 6(1)(f), and WP29 WP 217);
- Flexible change of purpose (Article 5(1)(b), WP29 WP 203);
- Expansive data minimisation (Articles 5(1)(c), 89(1));
- Flexible storage limitation (Articles 5(1)(e), 89(1));
- Enhanced security (Articles 5(1)(f), 32);
- Expansive further processing (Article 6(4), WP29 WP 217);
- Flexible profiling (WP29 WP 251 rev.01 - Annex 1, Recital 71, Article 22); and
- Ability to lawfully and ethically share, combine and enhance data (recitals 42 and 43, Articles 11(2), 12(2), WP29 WP259 rev.01).

The ENISA publication, *Recommendations on Shaping Technology According to GDPR Provisions: An Overview on Data Pseudonymisation*,[15] also highlights the following benefits of GDPR-compliant pseudonymisation:

1. Pseudonymisation serves as a vehicle to "relax" certain data controller obligations, including:

13 Additional information on GDPR compliant pseudonymisation is available at www.Pseudonymisation.com

14 The spirit of the GDPR is not to establish any techniques or technologies, as these could potentially not resist the proof of time. Rather, it deals with concepts such as data protection by design and by default, and appropriate technical and organisational safeguards. Consistent with the spirit of the GDPR, Pseudonymisation is presented not as a mere technique, but as an outcome.

15 See https://www.anonos.com/hubfs/ENISA_Pseudonymisation_Recomendations_GDPR_November_2018.pdf. Additional information on ENISA guidelines for GDPR compliant pseudonymisation is available at www.ENISAguidelines.com

a. Lawful repurposing (further processing) in compliance with purpose limitation principles;

b. Archiving of data for statistical processing, public interest, scientific or historical research;

c. Reduced notification obligations in the event of a data breach.

2. Pseudonymisation supports a more favourable (broader) interpretation of data minimisation.

3. Pseudonymisation goes beyond protecting "real-world personal identities" by protecting indirect identifiers.

4. Pseudonymisation provides for unlinkability between data and personal identity, furthering the fundamental data protection principles of necessity and data minimisation.

5. Pseudonymisation decouples privacy and accuracy, enabling Data Protection by Design and by Default while at the same time allowing data about individuals to remain more accurate.

"Data Embassy" Principles

The Data Embassy Principles, which are summarised at www.DataEmbassy.com, technically enforce established EU data protection principles to satisfy Schrems II requirements.

The Data Embassy Principles comprise:

1. **GDPR Pseudonymisation:** Enforcing GDPR-compliant Pseudonymisation[16] as per ENISA guidelines.[17] This is in accordance with the new standard set by GDPR Article 4(5) requirements to technically enforce WP29 and EDPS recommendations for Functional Separation.[18] Note that ***the effectiveness of these protections is able to be appealed by data subjects to an EU supervisory authority, ensuring the availability of effective judicial remedy under Article 47 of the EU Charter.***

2. **Data Minimisation:** Enabling Data Minimisation compliant with GDPR Article 5(1)(c) by enforcing Article 25(1) and 25(2) Data Protection by Design and by Default[19] requirements *using GDPR-compliant Pseudonymisation*.

3. **Secured Personal Data:** Restricting processing to a form of personal data that does not enable the identification of data subjects as provided under GDPR Articles 11(2) and 12(2) ***by keeping the "additional information" needed for relinking in the sole possession of the EU-based data exporter****.* This activates significant and far-reaching changes in a data controller's

16 Additional information on GDPR compliant pseudonymisation is available at www.Pseudonymisation.com

17 See Note 13, *Supra.*

18 See Notes 9 and 10, *Supra.*

19 Article 25 of the GDPR imposes new requirements for Data Protection by Design and by Default which means organisations must integrate or 'bake in' significant data protection capabilities into processing practices, from the design stage through the full data lifecycle. Previously known as 'Privacy by Design', this concept has long been part of data protection law. However, two key changes which are newly mandated under the GDPR are:

1. Legal mandate to support more than just privacy by design; Data Protection by Design and by Default requires the most stringent implementation of privacy by design; and
2. Heightened requirements, including the need to "implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation."

obligations that greatly facilitate "***compliance with the level of protection essentially equivalent to that guaranteed within the EU by the GDPR***."

Under GDPR Article 11(2), if the purposes for which an organisation processes personal data do not or no longer require identification of an individual, and if a data controller can show it is not in a position to identify data subjects and has, if possible, notified them of that fact, then it does not need to comply with the following data subject rights:

- Article 15 - Right of access by the data subject;
- Article 16 - Right to rectification;
- Article 17 - Right to erasure ('right to be forgotten');
- Article 18 - Right to restriction of processing;
- Article 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing; and
- Article 20 - Right to data portability;

Provided that under 11(2) the data subject may provide additional information enabling his or her identification for the purpose of exercising his or her rights.

Likewise, under GDPR Article 12(2), for similar reasons to those outlined for Article 11(2), a data controller again need not act on requests under Articles 15 to 20 as well as:

- Article 21 - Right to object, and
- Article 22 - Automated individual decision-making, including profiling, because of the nature of the protective measures in place.

4. **Demonstrability:** Proactive technical enforcement enables data controllers to demonstrate compliance with their accountability and demonstrability obligations under GDPR Article 5(2).

5. **Responsibility:** Technical and organisational measures enable data controllers to demonstrate compliance with their accountability and responsibility obligations under GDPR Article 24.

How Do The Data Embassy Principles Work (Technically)?

Traditional approaches to protecting privacy are analogous to "bathtub solutions." They work only so long as data use is limited to a confined place - a centralised location. They are not architected to be used outside of a confined place or a centralised location. When used outside of a confined place or a centralised location, their protections fail because the data becomes re-identifiable. In contrast, Data Embassy Principles allow data to be used outside of a confined place or a centralised location – analogous to data being available for privacy-respectful use "in the open ocean."

Data Embassy Principles provide a secured middle ground between the strongest data protection, and the highest level of data utility. Encryption affords maximum protection for data while at rest or in transit. However, encrypted data generally must be decrypted for use at which point it is not protected. Clear text data is the most valuable form of data, however, it has no protection. In contrast, GDPR Pseudonymisation-enabled Data Embassy Principles allow the protection of data *while* in use, and resolve the conflict between innovative data use and data protection.

In order to satisfy GDPR requirements for Pseudonymisation as an **outcome,** it is necessary to show that you cannot create links between the information value in the data and the actual identity of the data subject, without accessing the separately held “additional information” that is required for re-identification.

Conclusion

The implications of the Schrems II decision for SCCs and BCRs when data is transferred to countries without an adequacy decision are significant, and guidance to date suggests no grace period will be established. This means that organisations need to rapidly apply a solution that allows both compliance, and the continuation of global data transfers.

Data Embassy Principles, embodying Functional Separation and GDPR-defined Pseudonymisation, provide an appropriate “supplementary measure” for SCCs to comply with the requirements set forth in Schrems II. Applying Data Embassy Principles to data offers high quality data protection and privacy safeguarding, while preserving data utility and accuracy.