Schrems II Matrix for Compliant Data When in Use

ANONOS

State-of-the-art Pseudonymisation technology is commercially available today to enable Schrems II compliant processing by achieving "Aristotle's Golden Mean" of balancing between two extremes: *maximum data value and protection*. **GDPR Pseudonymisation is the most misunderstood and underutilised means of simultaneous data enablement and protection.** With it, organisations no longer need to engage in high-risk unlawful processing of data in the clear to achieve 100% accurate data innovation to achieve desired business outcomes.

Schrems II Compliance Requires All 7 Protections

GDPR-compliant Pseudonymisation is ***legally necessary**** because it is the only measure that satisfies all these data protection objectives to be less intrusive to fundamental rights.

	GDPR-compliant Pseudonymisation	Tokenisation (Pre-GDPR Pseudonymisation)	Encryption	Anonymisation	Differential Privacy	Synthetic Data	Homomorphic Encryption
1 Defeats Brute Force Attacks & Quantum Computing Risk.[1]	✓	✓	✗	✓	✓	✓	✗
2 Enables Protected Processing of Data When in Use.[2]	✓	✓	✗	✓	✓	✓	✓
3 Relinkable Only Under Controlled Conditions.[3]	✓	✓	✓	✗	✓	✗	✓
4 100% Accuracy vs Processing Unprotected Data in the Clear.[4]	✓	✗	✗	✗	✗	✗	✗
5 Accountable Reconciliation of Data Utility and Protection.[5]	✓	✗	✗	✗	✗	✓	✓
6 Protects Centralised and Decentralised Use Cases.[6]	✓	✗	✗	✓	✗	✓	✓
7 Defeats Unauthorised Re-Identification via the Mosaic Effect.[7]	✓	✗	✓	✓	✓	✓	✓

* Pseudonymisation is "legally necessary" under EU law when it is less intrusive to and more protective of rights under the GDPR and the EU Charter of Fundamental Human Rights than other data protection techniques. See European Court of Justice (ECJ) Case C-362/14, Schrems v. Data Protection Commissioner (October 2015 – "Schrems I"), and ECJ Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (July 2020 – "Schrems II").

1. EDPB Final Guidance paragraphs 83 and 89 and footnotes 80 and 81.
2. EDPB Final Guidance executive summary "...the protection granted to personal data in the European Economic Area (EEA) must travel with the data wherever it goes."
3. EDPB Final Guidance paragraphs 85, 94 and 96.
4. GDPR Article 5(1)(d). See also www.anonos.com/data-scientist-expert-opinion.
5. EDPB Final Guidance paragraphs 3, 4, 5 and 67.
6. EDPB Final Guidance executive summary "...the protection granted to personal data in the European Economic Area (EEA) must travel with the data wherever it goes."
7. EDPB Final Guidance paragraphs 79, 85, 86, 87, 88. See also https://mosaiceffect.com/

ANONOS

How Can Organisations Lawfully Process Data in the Cloud After Schrems II?

This document covers why GDPR-compliant Pseudonymisation is legally necessary for lawful cloud and remote processing of EU personal data. Why? Because it is less intrusive, more effective, and more privacy respectful than alternative data protection approaches.

State-of-the-art Pseudonymisation technology is commercially available today to enable Schrems II compliant processing by achieving "Aristotle's Golden Mean" of balancing between two extremes – maximum data value and protection. **Pseudonymisation is the most misunderstood and underutilised means of simultaneous data enablement and protection.** As a result, organisations need no longer engage in high-risk unlawful processing of data in the clear to achieve 100% accurate data innovation to achieve desired business outcomes.

This document is in three sections. The first is a 5-page summary, the second is an 18-page Epilogue to a University Dissertation, and the third (provided for background purposes only) is the original University Dissertation.

Table of Contents

ANONOS

How Can Organisations Lawfully Process Data in the Cloud After Schrems II?

I. **Summary of University Dissertation Highlighting Why Pseudonymisation is Necessary for Schrems II Compliant Cloud and Remote Processing of EU Personal Data** (4 pages)

The GDPR redefines Pseudonymisation, upgrading it from an ineffective anonymisation technique to a state-of-the-art data protection technical control providing better protection and better utility.

II. **Epilogue to Dissertation Reflecting Impact of Final EDPB Schrems II Guidance, Final European Commission Standard Contractual Clauses, and Increased Emphasis on Pseudonymisation** (18 pages)

The EDPB does not recognize encryption by itself as a lawful instrument of protection of data when utilizing cloud services or when having remote access to data stored in an inadequate third country, other than for the purpose of mere backup. Data pseudonymisation (implemented as defined in Use Case 2 and Article 4(5) GDPR), can be considered, among state-of-the-art technical safeguards available, to be the only lawful bridge available for transfers to third-country cloud service providers.

III. [Background] **Original Dissertation: Cross-Border Data Transfers and Data Localisation in The Aftermath of The Schrems II Judgement by Luigi Madaghiele** (62 pages)

The protection of data through effective technical measures could be the best method of protecting data while ensuring their free flow, independently of the regulatory framework of the third State.

How Can Organisations Lawfully Process Data in the Cloud After Schrems II?

I. Attached Dissertation Highlights Why GDPR Pseudonymisation is Necessary for Schrems II Compliant Cloud and Remote Processing of EU Personal Data

- Why did the European Data Protection Board (EDPP) increase the number of uses of Pseudonymisation from 7 times in their preliminary Schrems II guidance to 12 in the final Schrems II guidance (EDPB Final Guidance)?

- Why does the European Commission repeatedly highlight Pseudonymisation for Schrems II compliance generally, and specifically for completing Annex II to the final Standard Contractual Clauses (Final SCCs)?

- The attached dissertation (Dissertation) by an Italian university student shows that cloud and remote processing of EU personal data enabling data-driven business models are possible under Schrems II. Pseudonymisation – *as significantly redefined under the GDPR* – enforces purpose limitation, data minimisation, and other GDPR principles. **It is legally necessary because it is less intrusive, more effective, and more privacy respectful than alternative data processing approaches.**

Few organisations practice GDPR Pseudonymisation, which helps explain the widespread disbelief that the EDPB declared two popular use cases unlawful:

- **Use Case 6: Transfer of data in the clear to cloud services providers or other processors.**

- **Use Case 7: Transfer of personal data for business purposes including remote access.**

Organisations are asking, "How can cloud processing and remote access be unlawful (without GDPR Pseudonymisation) if (nearly) every organisation around the globe performs them daily?" The answer is found in the following statement by the Bavarian Data Protection Authority when announcing participation in the Schrems II investigation by German supervisory authorities:

> ***In many cases, the ECJ ruling requires a fundamental change in long-practiced business models and processes.***[1]

The Dissertation highlights disruptions to data supply chains when controllers and processors do not embrace "*fundamental change in long-practiced business models"* to comply with the ECJ position that **GDPR Pseudonymisation is "legally necessary" when it is less intrusive to and more protective of rights protected under the GDPR and the EU Charter of Fundamental Human Rights than other data protection approaches.**[2]

[1] An unofficial translation of the Bavarian Data Protection Authority press release announcing the investigation is available at https://www.anonos.com/hubfs/EDPB/Bavarian-DPA-Press-Release--Translated-to-English-by-Anonos.pdf

[2] See European Court of Justice (ECJ) Case C-362/14, Schrems v. Data Protection Commissioner (October 2015 – "Schrems I"), and ECJ Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (July 2020 – "Schrems II").

The Dissertation concludes:

> ***In the end, it may genuinely be inferred from these two Use Cases that the EDPB does not recognize encryption by itself as a lawful instrument of protection of data when utilizing cloud services or when having remote access to data stored in an inadequate third country, other than for the purpose of mere backup. Data pseudonymisation (implemented as defined in Use Case 2 and Article 4(5) GDPR), can be considered, among state-of-the-art technical safeguards available, to be the only lawful bridge available for transfers to third-country cloud service providers.***

The Dissertation outlines how the GDPR redefines Pseudonymisation, upgrading it from an ineffective anonymisation technique[3] to a state-of-the-art data protection technical control providing better protection and better utility.

GDPR Pseudonymisation enables organisations to evolve beyond current business practices of processing "Data in the Clear by Default" as represented by EDPB unlawful Use Case 6 and Use Case 7 to practising "Data Protection by Design and by Default" to achieve their business goals and objectives.

II. GDPR Pseudonymisation is the State-of-the-Art for Schrems II Compliance

The EDPB Final Guidance and the Commission's revised Final SCCs highlight GDPR Pseudonymisation as the state-of-the-art for Schrems II compliant data transfer, cloud, and remote access processing.
Why? **Because GDPR Pseudonymisation is "legally necessary" when it is less intrusive, more effective, and more privacy respectful than the following alternative data protection techniques.**

- **Tokenisation** (Pre-GDPR pseudonymisation): GDPR Pseudonymisation provides the benefit of protected processing in use but without the ease of re-identifying from correlating recurring (static) values within and among data sets when using pre-GDPR tokenisation (sometimes incorrectly referred to as pseudonymisation) to replace direct identifiers at the field-level only (the "Mosaic Effect").

- **Encryption:** GDPR Pseudonymisation provides the impenetrability of encryption, but without (i) vulnerability to brute force hacking/quantum computing of algorithmically derived schemes or (ii) the requirement to unprotect (decrypt) data and process it in the clear. Pseudonymisation uniquely protects data when in use.

[3] GDPR Pseudonymisation enables organisations to overcome the shortcomings of simple field-level pre-GDPR "pseudonymisation", which most people are familiar with (sometimes called key-coding or tokenisation), which is vastly inferior to GDPR Pseudonymisation because it involves only replacing direct identifiers and relies on static (persistent or recurring) tokens. The Article 29 Working Party 2014 Opinion on Anonymisation at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf highlighted the shortcomings of this outdated field-level approach to pre-GDPR pseudonymisation due to the ease with which data protected in such a manner can be re-identified. In contrast, the heightened requirements of GDPR Pseudonymisation enable organisations to protect data better than anonymisation because it allows them to replace indirect identifiers and attributes with tokens in a way that supports advanced analytics, artificial intelligence (AI) and machine learning (ML) to produce the same answer as when using unprotected cleartext. Anonymisation cannot achieve this result because, with anonymisation, organisations cannot reverse protection and use the results lawfully.

ANONOS

Schrems II Matrix for Compliant Data When in Use

State-of-the-art Pseudonymisation technology is commercially available today to enable Schrems II compliant processing by achieving "Aristotle's Golden Mean" of balancing between two extremes: *maximum data value and protection*. **GDPR Pseudonymisation is the most misunderstood and underutilised means of simultaneous data enablement and protection.** With it, organisations no longer need to engage in high-risk unlawful processing of data in the clear to achieve 100% accurate data innovation to achieve desired business outcomes.

Schrems II Compliance Requires All 7 Protections

GDPR-compliant Pseudonymisation is ***legally necessary**** because it is the only measure that satisfies all these data protection objectives to be less intrusive to fundamental rights.

© ANONOS 2021

	GDPR-compliant Pseudonymisation	Tokenisation (Pre-GDPR Pseudonymisation)	Encryption	Anonymisation	Differential Privacy	Synthetic Data	Homomorphic Encryption
1 Defeats Brute Force Attacks & Quantum Computing Risk.[1]	✓	✓	✗	✓	✓	✓	✗
2 Enables Protected Processing of Data When in Use.[2]	✓	✓	✗	✓	✓	✓	✓
3 Relinkable Only Under Controlled Conditions.[3]	✓	✓	✓	✗	✓	✗	✓
4 100% Accuracy vs Processing Unprotected Data in the Clear.[4]	✓	✗	✗	✗	✗	✗	✗
5 Accountable Reconciliation of Data Utility and Protection.[5]	✓	✗	✗	✗	✗	✓	✓
6 Protects Centralised and Decentralised Use Cases.[6]	✓	✗	✗	✓	✗	✓	✓
7 Defeats Unauthorised Re-Identification via the Mosaic Effect.[7]	✓	✗	✓	✓	✓	✓	✓

* Pseudonymisation is "legally necessary" under EU law when it is less intrusive to and more protective of rights under the GDPR and the EU Charter of Fundamental Human Rights than other data protection techniques. See European Court of Justice (ECJ) Case C-362/14, Schrems v. Data Protection Commissioner (October 2015 – "Schrems I"), and ECJ Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (July 2020 – "Schrems II").

1. EDPB Final Guidance paragraphs 83 and 89 and footnotes 80 and 81.
2. EDPB Final Guidance executive summary "...the protection granted to personal data in the European Economic Area (EEA) must travel with the data wherever it goes."
3. EDPB Final Guidance paragraphs 85, 94 and 96.
4. GDPR Article 5(1)(d). See also www.anonos.com/data-scientist-expert-opinion.
5. EDPB Final Guidance paragraphs 3, 4, 5 and 67.
6. EDPB Final Guidance executive summary "...the protection granted to personal data in the European Economic Area (EEA) must travel with the data wherever it goes."
7. EDPB Final Guidance paragraphs 79, 85, 86, 87, 88. See also https://mosaiceffect.com/

- **Anonymisation:** GDPR Pseudonymisation protects data from unauthorised reidentification like anonymisation (when the latter is done successfully, which is increasingly difficult and rare), but with (i) superior protection since you can protect both indirect as well as direct identifiers, and many attributes as well (when using anonymisation, protecting indirect identifiers and attributes renders data valueless due to the prohibition on reversing/relinking protected data), and (ii) increased value from the reversibility/relinkability of data under controlled conditions to enable authorised processing.

- **Differential Privacy:** GDPR Pseudonymisation provides the benefit of protected processing like differential privacy, but without (i) zero-sum "privacy budgets" forcing a trade-off between privacy and utility, requiring gains in privacy to come at the expense of utility, and (ii) being restricted to centralised applications. **GDPR Pseudonymisation enables both full protection and full utility, simultaneously, for both centralised and decentralised processing.**

- **Synthetic Data:** GDPR Pseudonymisation protects data from unauthorised reidentification like processing synthetic data, but (i) without incurring the delays required to regenerate data when data sets change or new data is incorporated, and (ii) with the additional benefit of being able to reverse and relink to identity under controlled conditions, which is not possible when using synthetic data.

- **Homomorphic Encryption:** GDPR Pseudonymisation provides the benefit of protected processing, but without the computational overhead and impracticability of homomorphic encryption for time-sensitive computational analysis.

III. What is Required for GDPR Pseudonymisation?

To satisfy statutory requirements, GDPR Pseudonymisation must fulfil the following to embed controls that travel with the data wherever it goes,[4] *including when in use*, to enable lawful transfer and processing when using SCCs by ensuring that the data does not reveal identity if third-party governments obtain access to it.

- **Protect all Personal Data:** GDPR Pseudonymisation must protect at the record and data set level by treating direct, quasi-, and indirect identifiers together with the unique behaviours or characteristics found in attributes that could be correlated with other data sources to reveal identity. This level of protection is very different from pre-GDPR techniques protecting only direct identifiers.[5]

- **Re-identification Risk Management at the Record/Data Set (vs Field) Level:** GDPR Pseudonymisation must enforce k-anonymity or other re-identification risk management checks at the record/data set level. When risk management checks are performed only at the field level, such as with pre-GDPR pseudonymisation, they do not protect against correlations among values within and between records enabling easy re-identification by correlating values via the Mosaic Effect.

- **Maximum Dynamism for Maximum Entropy:** GDPR Pseudonymisation does not use the same token to replace different occurrences of the same value across data sets. Instead, whenever possible, different tokens are dynamically assigned to replace the same value at different times for various purposes to prevent the re-identification of individuals via the Mosaic Effect. In this manner, GDPR Pseudonymisation establishes maximum entropy (uncertainty) between data sets, so the data is "anonymous" (in the strictest sense of the word on a global basis) **"but for"** the additional information which is held separately by the controller.

- **Non-Algorithmically Derived Look-up Tables.** The EDPB Final Guidance recommends table look-up mechanisms for GDPR Pseudonymisation versus the exclusive use of cryptography for creating tokens, thereby overcoming the risk of brute-force unauthorised re-identification by dynamically substituting uncorrelated Pseudonyms for original data.[6]

- **Accountability.** To comply with accountability and demonstrability obligations under GDPR Article 5(2) and responsibility obligations under Article 24, data controllers and processors must ensure the consistent, scalable, predictable, and auditable enforcement of the preceding GDPR Pseudonymisation requirements so that data is not re-identifiable other than by using additional information kept separately by the controller.

[4] The executive summary of the EDPB Final Guidance states "In its recent judgment C-311/18 (Schrems II) the Court of Justice of the European Union (CJEU) reminds us that the protection granted to personal data in the European Economic Area (EEA) *must travel with the data wherever it goes*."
[5] Supra, Note 3.
[6] EDPB Final Guidance paragraphs 83 and 89 and footnotes 80 and 81.

IV. Benefits of GDPR Pseudonymisation Under Schrems II

GDPR Pseudonymisation enables organisations to support lawful processing by establishing *by default* the use of data protection respectful GDPR Pseudonymised data whenever and wherever possible (as required by GDPR Article 25 Data Protection by Design and by Default and GDPR Article 32 Security of Processing) so that unprotected non-GDPR Pseudonymised (i.e., identifying) data is processed only when necessary (helping to satisfy GDPR Articles 5(1)(b) Purpose Limitation and 5(1)(c) Data Minimisation obligations), and only where:

- There is a legal basis to do so under Article 6 (e.g., based on Article 6(1)(a) consent, 6(1)(b) contract, or 6(1)(f) legitimate interests by leveraging Pseudonymisation-enabled technical and organisational measures to satisfy the "balancing of interests" test); and

- The processing satisfies derogation requirements (e.g., Article 49(1)(a) based on consent, Articles 49(1)(b) or (c) based on contract).

V. GDPR State-of-the-Art Requirements

- Controllers and processors are obligated to take into account the state-of-the-art when fulfilling their data protection obligations under the GDPR.[7]

- The Dissertation highlights that:

    - GDPR Pseudonymisation is the state-of-the-art in technical safeguards and is the only lawful bridge available for Schrems II compliant use of third-country cloud service providers; and

    - Anonos Data Embassy® software is the state-of-the-art in GDPR Pseudonymisation.

[7] See GDPR Recital 78 and Articles 25 (Data Protection by Design and by Default) and 32 (Security of Processing).

How Can Organisations Lawfully Process Data in the Cloud After Schrems II?

I. **Summary of University Dissertation Highlighting Why Pseudonymisation is Necessary for Schrems II Compliant Cloud and Remote Processing of EU Personal Data** (4 pages)

The GDPR redefines Pseudonymisation, upgrading it from an ineffective anonymisation technique to a state-of-the-art data protection technical control providing better protection and better utility.

II. **Epilogue to Dissertation Reflecting Impact of Final EDPB Schrems II Guidance, Final European Commission Standard Contractual Clauses, and Increased Emphasis on Pseudonymisation** (18 pages)

The EDPB does not recognize encryption by itself as a lawful instrument of protection of data when utilizing cloud services or when having remote access to data stored in an inadequate third country, other than for the purpose of mere backup. Data pseudonymisation (implemented as defined in Use Case 2 and Article 4(5) GDPR), can be considered, among state-of-the-art technical safeguards available, to be the only lawful bridge available for transfers to third-country cloud service providers.

III. [Background] **Original Dissertation: Cross-Border Data Transfers and Data Localisation in The Aftermath of The Schrems II Judgement by Luigi Madaghiele** (62 pages)

The protection of data through effective technical measures could be the best method of protecting data while ensuring their free flow, independently of the regulatory framework of the third State.

20 July 2021

EPILOGUE TO DISSERTATION ON CROSS-BORDER DATA TRANSFERS AND DATA LOCALISATION IN THE AFTERMATH OF THE SCHREMS II JUDGEMENT

By Luigi Madaghiele[1]

This Epilogue is meant to update my dissertation, CROSS-BORDER DATA TRANSFERS AND DATA LOCALISATION IN THE AFTERMATH OF THE SCHREMS II JUDGEMENT (the "Dissertation")[2], to reflect the impact of three events following submission of my Dissertation to the University of Trento[3] with respect to following concluding point of my Dissertation:

> **[T]he protection of data through effective technical measures could be the best method of protecting data while ensuring their free flow, independently of the regulatory framework of the third State.**

SUMMARY

The three events, which collectively highlight the mandate under Schrems II to transform legal requirements into technical measures that combine enhanced security and data protection controls, are the following:

1. **EDPB FINAL GUIDANCE:** Adoption by the European Data Protection Board (EDPB) of Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data Version 2.0 on 18 July 2021 ("EDPB Final Guidance").[4]

   A. Expanded Flexibility for Derogations

   B. Intra-EEA Processing Obligations

   C. Preference for Non-Algorithmically Derived Pseudonyms

2. **FINAL SCCs:** Adoption by the European Commission of the Implementing Decision (EU) 2021/914 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on 4 June 2021 ("Final SCCs").[5]

   A. Supplementary Measures Required for Data Supply Chains

   B. Technically Enforced Common Threshold of Protection

   C. Supplementary Measures Required for Existing as well as New SCCs

[1] Master of Science student in Law, Digital Innovation and Sustainability at LUISS Guido Carti University, Graduate in Comparative, European and International Legal Studies from the University of Trento, Erasmus exchange in Global Law at Tilburg University.
[2] A copy of the Dissertation, as updated by this Epilogue, is available at www.SchremsII.com/Epilogue.
[3] The University of Trento is one of the top 10 ranked universities in Italy, top 100 universities in Europe, and top 225 universities globally. For more information, see www.usnews.com/education/best-global-universities/university-of-trento-504044 and www.unitn.it/en/ateneo/1636/rankings.
[4] See https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
[5] See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN

3. **INCREASED EMPHASIS ON PSEUDONYMISATION:** There was a significant increase in references to Pseudonymisation in the EDPB Final Guidance. For this reason, I conducted further research into Pseudonymisation and introduced myself to and had discussions with Magali Feys and Gary LaFever[6], the authors of the Pseudonymisation-enabled "Data Embassy Principles" memorandum submitted to the EDPB[7], cited in footnotes 210 and 211 of my Dissertation (the "Data Embassy Memorandum").

   A. Lack of Pseudonymisation Makes EDPB Use Case 6 and 7 Unlawful

   B. Benefits of EDPB Lawful Use Case 2 – Transfer of Pseudonymised Data

   C. GDPR Pseudonymisation Superior to Anonymisation

   D. Three Schrems II Use Cases for GDPR Pseudonymisation

      (i) Expanded Flexibility for Derogations

      (ii) Intra-EEA Processing Obligations

      (iii) Preference for Non-Algorithmically Derived Pseudonyms

DETAILED ANALYSIS

1. EDPB FINAL GUIDANCE

After submitting my Dissertation to the University of Trento, the EDPB finalised its guidance on 'supplementary measures', which includes significant changes from the preliminary guidance cited in footnote 80 and 84 of my Dissertation. The screenshots[8] below highlight differences between the EDPB's preliminary and final guidance.[9]

A. Expanded Flexibility for Derogations

Changes to the Final EDPB Guidance from the preliminary version (highlighted in the screenshots below) show greater flexibility in using derogations than initially noted in my Dissertation. To the extent that the requirements cited in footnote 100 of the Dissertation[10] are followed, derogations under Article 49 are available to serve as "*exemptions from the general principle that personal data may only be transferred to third countries if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights in order to continue to benefit from*

[6] See https://www.dataembassy.com/
[7] See https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/edpb_data_embassy_memorandum_-_11_november_2020.pdf
[8] See https://www.linkedin.com/posts/piracybydesign_redline-edpb-recommendations-012020-ugcPost-6812701015935082496-i6YT for the source of the screenshots used in this Epilogue.
[9] For all screenshots in this Epilogue, red stricken text indicates deletions, blue underlined text indicates additions, and green underlined text denoted text moved from one place to another between preliminary drafts and final versions.
[10] See Guidelines 2/2018 of the European Data Protection Board of 25 May 2018 on Derogations of Article 49 under Regulation 2016/679 at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

their fundamental rights and safeguards" so long as "*the derogations [are] interpreted restrictively so that the exception does not become the rule*."[11]

Considering that such derogations are meant to be interpreted restrictively and can only be invoked where all the derogations requirements[12] are met, the EDPB considered that a restriction of their use for "regular and repetitive" purposes would be rather excessive. The Final EDPB Guidance, therefore, no longer constrains derogations from use for "regular and repetitive" purposes, so long as they are limited to "specific situations", and this constitutes a significant change.

A **second step** is to **verify the transfer tool your transfer relies on**, amongst those listed under Chapter V GDPR. If the European Commission has already declared the country, region or sector to which you are transferring the data as adequate, through one of its adequacy decisions under Article 45 GDPR or under the previous Directive 95/46 as long as the decision is still in force, you will not need to take any further steps, other than monitoring that the adequacy decision remains valid. In the absence of an adequacy decision, you need to rely on one of the transfer tools listed under Articles 46 GDPR ~~for transfers that are regular and repetitive~~. Only in some cases ~~of occasional and non-repetitive transfers~~ you may be able to rely on one of the derogations provided for in Article 49 GDPR~~,~~ if you meet the conditions. Derogations cannot become "the rule" in practice, but need to be restricted to specific situations.

Derogations

24. Besides adequacy decisions and Article 46 GDPR transfer tools, the GDPR contains a third avenue allowing transfers of personal data in certain situations. Subject to specific conditions, you may still be able to transfer personal data based on a derogation listed in Article 49 GDPR.

25. Article 49 GDPR has an exceptional nature. The derogations it contains must be interpreted ~~restrictively and mainly relate to processing activities that are occasional and non-repetitive.~~in a way which does not contradict the very nature of the derogations as being exceptions from the rule that personal data may not be transferred to a third country unless the country provides for an adequate level of data protection or, alternatively, appropriate safeguards are put in place. Derogations cannot become "the rule" in practice, but need to be restricted to specific situations. The EDPB has issued its Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/~~679.36~~679.37

26. Before relying on an Article 49 GDPR derogation, you must check whether your transfer meets the strict conditions this provision sets forth for each of them.

B. Intra-EEA Processing Obligations

As highlighted in the screenshots below, technical supplementary measures are required under the GDPR antecedent to Schrems II requirements for lawful international data transfers. Much of the processing comprising popular "Big Data" practices must satisfy explicitly defined "legitimate interest" processing requirements to be legally permissible under the GDPR.[13] In addition, GDPR Article 25 (on *Data Protection by Design and by Default*) and 32 (on *Security of*

[11] Id at page 4.
[12] See section 3(D)(i) of this Epilogue.
[13] See www.anonos.com/legitimate-interest

processing) explicitly require the use of technology to mitigate risks to data subjects (both Articles 25 and 32 specifically highlight Pseudonymisation). The requirements for establishing a lawful basis for processing under Article 6 (e.g., Legitimate Interests) and those from Articles 25 and 32 are **mandatory for all processing,** which self-evidently encompasses processing localised solely within the European Economic Area (EEA) or adequacy countries.

> ~~71~~76. As a controller or processor, you may already be required to implement some of the measures described in this annex~~, even if your~~ in order to be compliant with the GDPR. This means similar measures might need to be put in place for personal data processed in the EEA, transferred to a data importer ~~is~~ covered by an adequacy decision, ~~just as you may be required to implement them when you process data within the EEA.[66]~~ or to other third countries.[77]
>
> ~~78~~83. Controllers may have to apply some or all of the measures described here irrespective of the level of protection provided for by the laws applicable to the data importer because they are needed to comply with Articles 25 and 32 GDPR in the concrete circumstances of the transfer. In other words, exporters may be required to implement the measures described in this paper even if their data importers are covered by an adequacy decision, just as controllers and processors may be required to implement them when data is processed within the EEA.

C. Preference for Non-Algorithmically Derived Pseudonyms

The Final EDPB Guidance expresses concern over the risks to current data protection technology to withstand advances in cryptanalytic techniques, the emergence of new computing paradigms like quantum computing and the increasing availability of computing capabilities. Similar concerns undergirded the following closing statement in Chapter 3.2 of my Dissertation, "Cloud Services and Their Post-Schrems II Challenges: Reconciling Data sovereignty and Data Flows":

> *"What is foreseeable is that technical data protection standards will improve, also as a consequence of Schrems II and its additional safeguards clause. The use of techniques like pseudonymisation, nonetheless, is threatened by a disruptive innovation: quantum computing. With its enormous computing power, it is expected to shake all the grounds on which we are standing now as far as concerns techniques of data securitization."*

The screenshots below from the Final EDPB Guidance highlight this concern. Footnote 80 and 81, referring to Use Case 1 on encryption-secured data transferred for merely storage purposes, already signal the necessity of state-of-the-art technology (which is generally "subject to decline over time" for the reasons stated above) being set up in order to achieve compliance. This motivated the EDPB to express their preference for non-algorithmically derived pseudonymisation look-up tables (when referring to Use Case 2), held separately and securely in the EU as a means of thwarting unauthorised attempts at brute-force reidentification.

[80] For the assessment of the strength of encryption algorithms, their conformity with the state-of-the-art, and their robustness against cryptanalysis over time, data exporters can rely on technical guidance published by official cybersecurity authorities of the EU and its member states. See e.g. ENISA Report « What is "state of the art" in IT security? », 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it- security; guidance given by the German Federal Office for Information Security in its Technical Guidelines of the TR-02102 series and "Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018" at https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81] The protective capacity of cryptographic algorithms is subject to decline over time due to the discovery of new cryptanalytic techniques, the emergence of new computing paradigms like quantum computing, and the general increase of available computing power, unless the applied algorithms are proven to be information theoretically secure. This concern applies in particular to public key algorithms that are at the time of writing in common use. In consequence, the data exporter has to consider that public authorities may undertake to access encrypted data in the circumstances described in paragraph No. 80, and store it until their resources are sufficient for decryption. The supplementary measure can only be considered effective if such decryption and subsequent further processing at that time would no longer constitute an infringement of the rights of data subjects, e.g., because the data can no longer be used to directly or indirectly identify them.

Use Case 2: Transfer of pseudonymised Data

~~80~~85. A data exporter first pseudonymises data it holds, and then transfers it to a third country for analysis, e.g., for purposes of research.

If

1. a data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group~~,~~ without the use of additional information[~~69~~],[83]
2. that additional information is held exclusively by the data exporter and kept separately in a Member State or in a third country, ~~territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate~~by an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection ~~is ensured~~to that guaranteed within the EEA,
3. disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards, it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information, and
4. the controller has established by means of a thorough analysis of the data in question - taking into account any information that the public authorities of the recipient country may be expected to possess and use - that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information,

then the EDPB considers that the pseudonymisation performed provides an effective supplementary measure.

[83] In line with Article 4(5) GDPR: "'pseudonymisation' means 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;" Additional data may consist of tables juxtaposing pseudonyms with the identifying attributes they replace, cryptographic keys or other parameters for the transformation of attributes, or other data permitting the attribution of the pseudonymised data to identified or identifiable natural persons.

89. If, in the course of performing pseudonymisation, attributes contained in the personal data are transformed using a cryptographic algorithm, then the guidance in footnotes 80 and 81 applies. Henceforth it is recommended to forego the exclusive use of cryptography, and apply transformations based on table look-up mechanisms.

2. FINAL SCCs

A. Supplementary Measures Required for Data Supply Chains

The following provisions in the Final SCCs highlight the importance to **all participants in "data supply chains"** (i.e., all data controllers, co-controllers, processors, and sub-processors involved in specific data transfers) to require that all parties **implement adequate technical and organisational measures** to avoid risk of liability and termination of data flows (emphasis added):

a. All data exporters must warrant that they used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under the SCCs.[14]

b. Technical and organisational measures must be described in detail and not in general terms and must consider "*the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner*."[15]

c. *"[I]n case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter*."[16]

d. Clause 12 imposes **joint and several liability on all parties in data supply chains**.[17] This means that data subjects can recover all of their losses from any one of the multiple parties in a data supply chain (e.g., the initial data source or controller, any co-controller, processor or sub-processor) leaving it up to the data supply chain parties to clarify amongst themselves which party(s) should bear what portion of the liability - but only after the data subject has received a full recovery for "*any material or non-material damages*".[18] Furthermore, "The data importer may not invoke the conduct of a sub-processor to avoid its own liability."[19]

[14] Clause 8 of the Final SCCs.
[15] Id.
[16] Id.
[17] These obligations are consistent with those under Article 82 of the GDPR.
[18] Clause 12 of the Final SCCs.
[19] Id.

Appropriate technical and organisational measures, such as encryption and pseudonymisation, are required for SCCs to be lawful because contractual terms do not bind the authorities of third countries. In other words, the validity and effectiveness of SCCs depends on whether supplementary measures can ensure an adequate level of protection.[20] If supplementary measures are incapable of compensating for a lower threshold of data protection, operators and processors must suspend or terminate transfers.[21]

Activity in Germany provides a real-world example of the importance of supplementary measures for avoiding operational risk from disruptions to data flows. A task force of German supervisory authorities initiated Schrems II enforcement investigations by sending questionnaires to German data controllers[22], highlighting that SCCs are lawful for data transfers subject to FISA Section 702 only if supplemented with adequate additional safeguards. Question 9 of the German questionnaire specifically asks what supplementary measures have been implemented[23] In response, German automobile manufactures, financial services, pharmaceutical and telecommunications data controllers have begun requesting parties in their "data supply chain" to answer the same question regarding what supplementary measures exist. If downstream data supply chain partners do not have adequate safeguards, upstream data controllers and processors may prefer to discontinue data flow rather than risk damage to their businesses.

B. Technically Enforced Common Threshold of Protection

Considering the above, the following excerpts from Section 2.2 of my Dissertation, "Legal Bases for Data Transfers in the Aftermath of Schrems II and Their Implementation", highlight the importance to EU data exporters of establishing a common threshold of protection by implementing technical safeguards that ensure EU equivalent protection independent of the regulatory framework of any third country, notwithstanding the lack of assistance from cloud or other technology providers:

> *"…a majority of companies both established in the US[24] and in the EU[25] expressed an intention not to comply with the judgement. Among these it was possible to find Microsoft and Amazon Web Services[26], the main cloud computing services providers in the world[27].*
>
> *A partner of the company that issued the survey has noted how, instead, businesses that want to be compliant will address the changes in the framework of data transfers:*

[20] CJEU, C-311/18, Schrems II, para. 125.
[21] In the Schrems II ruling, the CJEU notes five times that the appropriate remedy for failing to comply with international data transfer requirements is injunctive relief suspending or terminating transfers (see paragraphs 121, 135, 146, 154, and 203(3) of the ruling).
[22] See EDPB press release announcing coordinated German investigation of international data transfers at https://edpb.europa.eu/news/national-news/2021/coordinated-german-investigation-international-data-transfers_en. An unofficial translation of the press release issued by the Bavarian State Office for Data Privacy Protection announcing the investigation is available at www.SchremsII.com/Bavarian-DPA-Press-Release.
[23] An unofficial translation of the questionnaire sent by participating German supervisory authorities, specifically targeting Intra-Group Data Traffic, is available at www.SchremsII.com/German-DPA-Questionnaire.
[24] Nielsen, Nikolai. 2020. "US Firms Ignoring EU Court Ruling on Data, Schrems Warns." EUobserver. September 4, 2020. https://euobserver.com/justice/149329.
[25] Klovig Skelton, Sebastian. 2020. "Over Half of Firms Intend to Continue US Data Transfers despite Schrems II." ComputerWeekly.Com. September 23, 2020. https://www.computerweekly.com/news/252489498/Over-half-of-firms-intend-to-continue-US-data-transfers-despite-Schrems-II.
[26] "Schrems II Hub: Every Development in the Saga." n.d. Global Data Review. Accessed May 26, 2021. https://globaldatareview.com/data-localisation/schrems-ii-hub-every-development-in-the-saga.
[27] Jones, Edward. 2021. "AWS vs Azure in 2021 (Comparing the Cloud Computing Giants)." Kinsta. March 25, 2021. https://kinsta.com/blog/aws-vs-azure/.

many will just skip the transfer impact assessment, and will only assume that any State they plan to send the data to will simply not provide equivalent protections to the EU. The required case-by-case assessment is not necessary if the threshold allowing the transfer is set always at the same level, that is, a level equivalent to the EU.[28]"

The technical enforcement of SCCs before submitting EU personal data for cloud-based analytics, artificial intelligence (AI) or machine learning (ML) processing by using GDPR-compliant Pseudonymisation to protect the data when in use would reduce the effort required for case-by-case risk assessment required by Schrems II, since even in the worst-case situation the protection could safeguard equivalent data subjects' rights to privacy and data protection.[29]

C. Supplementary Measures Required for Existing as well as New SCCs

The CJEU Schrems II ruling requiring appropriate technical and organisational measures, such as encryption and pseudonymisation, for SCCs to be lawful is not limited to new SCCs. EU data exporters are obliged to implement such measures to support SCCs – **both existing and new** – to comply with Schrems II requirements. This obligation was immediate on the date of the Schrems II ruling over a year ago and, no grace period has ever been provided. As a consequence, transfers of data to inadequate third countries reliant on the old SCCs not supplemented by the required additional safeguards have been since the day of the Schrems II judgement unlawful. The enactment of the new SCCs did not erase the requirement for additional safeguards; on the contrary, it restated and strengthened such obligation with the provisions highlighted in paragraph A of this Chapter.

Overall, nothing in the EDPB Final Guidance nor in the Final SCCs contravenes the following restatement of the immediacy of this obligation by the EDPB in its 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:[30]

"3) Is there any grace period during which I can keep on transferring data to the U.S. without assessing my legal basis for the transfer?

No, the Court has invalidated the Privacy Shield Decision without maintaining its effects, because the U.S. law assessed by the Court does not provide an essentially equivalent level of protection to the EU. This assessment has to be taken into account for any transfer to the U.S."

3. INCREASED EMPHASIS ON PSEUDONYMISATION

A. Lack of Pseudonymisation Makes EDPB Use Case 6 and 7 Unlawful

An increased emphasis on pseudonymisation for complying with Schrems II requirements is indisputable. In addition to the references to pseudonymisation noted above, it is telling to note that while there were 7 references to pseudonymisation in the preliminary EDPB Schrems II guidance in November 2020, there were nearly double that number (i.e., 12) in the Final EDPB Guidance.

[28] Klovig Skelton, 2020. "Over Half of Firms Intend to Continue US Data Transfers despite Schrems II".
[29] Id.
[30] See https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

The screenshots from the Final EDPB Guidance copied below highlight that the omission or unavailability of pseudonymisation for protecting data *when in use* (as noted in EDPB Lawful Use Case 2[31] versus **encryption** which **only protects data when at rest or in transit (but not *when in use***) as highlighted in EDPB Lawful Use Case 1 and 2) is explicitly a primary reason for the unlawfulness of both Use Case 6 - *Transfer to Cloud Services Providers or Other Processors Which Require Access to Data in the Clear*[32] and Use Case 7 - *Transfer of Personal Data for Business Purposes Including by Way of Remote Access*.[33]

Unlawful Use Case 6 - *Transfer to Cloud Services Providers or Other Processors Which Require Access to Data in the Clear*

8894. A data exporter ~~uses~~transfers personal data, whether by electronic transmission or by making it available to a cloud service provider or other processor to have personal data processed according to its instructions in a third country~~.~~ (e.g., for the provision of technical support or any type of cloud processing), and this data is not - or cannot- be pseudonymised as described in Use Case 2 or encrypted as described in Use Case 1 because the processing requires accessing data in the clear.

Unlawful Use Case 7 - *Transfer of Personal Data for Business Purposes Including by Way of Remote Access*

9096. A data exporter ~~makes~~transfers personal data ~~available~~ to entities - in a third country to be used for shared business purposes~~. A~~ —whether by electronic transmission or by making it available to remote access by the data importer—, and this data is not - or cannot- be -pseudonymised as described in Use Case 2 or encrypted as described in Use Case 1 because the processing requires accessing data in the clear. One typical constellation may consist of a controller or processor established on the territory of a Member State transferring personal data to a controller or processor in a third country belonging to the same group of undertakings, or group of enterprises engaged in a joint economic activity. The data importer may, for example, use the data it receives to provide personnel services for the data exporter for which it needs human resources data, or to communicate with customers of the data exporter who live in the European Union by phone or email.

In the end, it may genuinely be inferred from these two Use Cases that the EDPB does not recognize encryption by itself as a lawful instrument of protection of data when utilizing cloud services or when having remote access to data stored in an inadequate third country, other than for the purpose of mere backup. Data pseudonymisation (implemented as defined in Use Case 2 and Article 4(5) GDPR), can be considered, among state-of-the-art technical safeguards available, to be the only lawful bridge available for transfers to third-country cloud service providers.

[31] See paragraph 85 et seq of EDPB Final Guidance.
[32] See paragraph 94 et seq of EDPB Final Guidance.
[33] See paragraph 96 et seq of EDPB Final Guidance.

B. Benefits of EDPB Lawful Use Case 2 – Transfer of Pseudonymised Data

Despite numerous references to pseudonymisation under both the Final SCCs and the EDPB Final Guidance for compliance with Schrems II requirements, a surprising the number of commentators and articles mention only encryption, or mischaracterize the capabilities of pseudonymisation (i.e., describing pseudonymisation as merely a technique instead of the resulting characteristic of a properly transformed dataset pursuant to the express requirements of GDPR Article 4(5) and the EDPB Final Guidance).[34]

To gain greater clarity about Pseudonymisation, I contacted Magali Feys and Gary LaFever at Anonos[35], the authors of the Data Embassy Memorandum[36] cited in my Dissertation which influenced recognition by the EDPB of Lawful Use Case 2 – Transfer of Pseudonymised data, by highlighting the ability of GDPR Pseudonymisation to enable equivalent protection in compliance with Schrems II requirements. I learned many things from Ms. Feys and Mr. LaFever. For example, while Anonos changed the name of its technology to "Data Embassy" in connection with the Schrems II judgement,[37] the software is the result of over 8 years and tens of thousands of hours of legal and technical research and development. The commitment by Anonos to inventing and implementing state-of-the-art technology for reconciling conflicts between data security, protection and innovation is evidenced by the following achievements:

- Anonos technology is the only technology certified as complying with GDPR Pseudonymisation requirements[38].

- Anonos "Best Practices" for Schrems II compliant transfers are included in the Code of Conduct for Pseudonymisation submitted to the EDPB by the German Association for Data Protection and Data Security ("GDD" or Gesellschaft für Datenschutz und Datensicherheit e.V.).[39]

- Anonos Data Embassy software complies with all 50 of the GDPR-compliant Pseudonymisation Best Practices derived by Anonos after careful study and analysis of these reports by the European Union Agency for Cybersecurity (ENISA):[40]
    - *ENISA: Pseudonymisation Techniques and Best Practices* (2018);
    - *ENISA: Recommendations on Shaping Technology According to GDPR Provisions* (2019); and
    - *ENISA: Data Pseudonymisation: Advanced Techniques and Use Cases* (2021).

[34] For example, see https://iapp.org/news/a/uncertainty-aplenty-a-year-after-schrems-ii-ruling/, *https://www.cato.org/blog/tiktok-schrems-ii-cross-border-data-flows, and https://www.mintz.com/insights-center/viewpoints/2826/2021-06-22-eu-data-protection-regulators-adopt-guidance-personal*

[35] www.anonos.com

[36] https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/edpb_data_embassy_memorandum_-_11_november_2020.pdf

[37] The capabilities of Anonos software, previously branded as "Big Privacy", to satisfy GDPR and Schrems II requirements are highlighted in an IDC report titled "Embedding Privacy and Trust Into Data Analytics Through Pseudonymisation," available at *https://www.anonos.com/hubfs/Embedding_Trust_Into_Data_Anonos_IDC_August_2020.pdf?hsLang=en*. Anonos changed the name of its software from "Big Privacy" to "Data Embassy" because when travelling in a foreign country, travelers can turn to their home country's embassy for predictable protection and physical security. Anonos reasoned that similarly, its Data Embassy software embeds protection and physical security into data no matter "where it travels" or what country it is in.

[38] https://repository.europrivacy.org/en/certifications/edit/3ae8d3f2-d129-11e8-8e66-000c29bba468

[39] www.Anonos.com/TenTruths

[40] https://www.enisaguidelines.com/

C. GDPR Pseudonymisation is Superior to Anonymisation for Schrems II and for GDPR Compliance

Anonos maintains numerous educational resources on GDPR-compliant Pseudonymisation, including:

- www.pseudonymisation.com
- www.anonos.com/gdpr-pseudonymisation-benefits
- www.dataembassy.com
- www.mosaiceffect.com
- www.enisaguidelines.com
- www.anonos.com/legitimate-interest
- www.anonos.com/anonymisation-under-the-gdpr
- www.anonos.com/data-scientist-expert-opinion
- www.anonos.com/TenTruths
- Schrems_II_LinkedIn_Group

The following "**7 Benefits of GDPR Pseudonymisation**" were developed by Anonos to highlight the advantages of Pseudonymisation over anonymisation under the GDPR and Schrems II.

1. For data to be truly "anonymous" under the GDPR, the data must not be capable of being cross-referenced with other data to reveal identities of data subjects, "both by the controller or any other person."[41] This necessarily includes deletion of source data[42]. This very high standard is required because when data satisfies the requirements for anonymisation, it is deemed to be outside the scope of fundamental rights protection under the GDPR.

   In today's world of Big Data processing, data held by a controller is often linkable with data that is beyond the control of the controller thereby facilitating unauthorized re-identification and exposing:

   - The data controller to potential liability.
   - Data sharing partners of the controller to potential liability.
   - Data subjects to potential violations of their fundamental rights.

2. Under the GDPR and Final EDPB Guidance, the term Pseudonymisation requires a new "state" of data, including:

   - Protection of direct, indirect, and quasi-identifiers, together with characteristics and behaviours;

[41] GDPR Recital 26.
[42] See footnote 2 of the Final SCCs stating that anonymisation "requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible." See also www.anonos.com/anonymisation-under-the-gdpr

- Protection at the record and data set level versus only the field level so that the protection travels wherever the data goes, including when it is in use; and

- Dynamic generation of high entropy levels (uncertainty) to defeat unauthorised re-identification by assigning different tokens at different times for various purposes.

The foregoing protections are necessary to prevent the re-identification of data subjects without the use of additional information kept separately, as required under Article 4(5)[43] and as further underscored by paragraph 85(4) of the EDPB Final Guidance.[44] GDPR Pseudonymisation essentially requires that data is "anonymous" (in the strictest EU sense of the word - globally anonymous) "but for" the additional information held separately and made available under controlled conditions as authorised by the data controller for permitted re-identification of individual data subjects.[45]

3. Simple field-level "pseudonymisation", which most people are familiar with (sometimes called key-coding or tokenisation), is vastly inferior to GDPR-compliant pseudonymisation because it involves only replacing direct identifiers with static (persistent or recurring) tokens. The Article 29 Working Party 2014 Opinion on Anonymisation[46] highlights the shortcomings of this now outdated approach to pseudonymisation due to the ease with which data protected in such a manner can be re-identified.

4. One of the biggest misunderstandings under the GDPR is the lack of appreciation for how significantly the definition of Pseudonymisation is elevated and heightened.[47] In addition to 100% precision relative to processing the corresponding cleartext, Pseudonymised data processes as quickly as cleartext. In contrast, synthetic data must be recalibrated each time data, users or use cases are changed to reflect new data interrelationships, increasing elapsed processing time by 4X or more depending on the level of variability between data sets. Worse, homomorphic encryption and blockchain can take days to process advanced calculations processed in seconds using cleartext or Pseudonymisation.

5. Pseudonymisation protects data better than anonymisation because Pseudonymisation enables you to replace indirect identifiers and attributes with tokens in a way that enables you to perform advanced analytics, artificial intelligence (AI) and machine learning (ML) to produce the same answer as when using unprotected cleartext. Anonymisation cannot achieve this result because with anonymisation you are not able to lawfully reverse protection and make use of the results. In contrast, Pseudonymisation enables 100% retained value and utility[48] because you are explicitly permitted to reverse

[43] Article 4(5) of the GDPR defines Pseudonymisation as "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."
[44] Paragraph 85(4) of the Final EDPB Guidance requires that "the controller has established by means of a thorough analysis of the data in question – taking into account any information that the public authorities of the recipient country may be expected to possess and use – that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information."
[45] See www.enisaguidelines.com, www.pseudonymisation.com, www.dataembassy.com, and www.mosaiceffect.com
[46] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[47] See the Ten Truths of Pseudonymisation discussed by Steffen Weiss, legal counsel for the German Association for Data Privacy and Data Security (GDD) and Gary LaFever, Anonos CEO and General Counsel at www.anonos.com/TenTruths
[48] See https://www.anonos.com/data-scientist-expert-opinion

protection under controlled conditions for authorised processing. This provides greater protection and utility than anonymisation which is caught in a catch-22 because it cannot replace identifiers with reversible tokens; to do so results in data that can be re-identified and is not anonymous.

6. Pseudonymisation is recommended as a technical supplementary measure for Schrems II compliance (both by the EU Commission and the EDPB) whereas anonymisation is not. In fact, as highlighted in the screenshot below, anonymisation was eliminated from the Final SCCs (versus being included the preliminary draft) for reasons such as those enumerated above.

~~1.6~~8.6 Security of processing

(a) The data importer and, during ~~the~~ transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, ~~they~~the Parties shall take due account of the ~~risks involved in the processing,~~state of the art, the costs of implementation, the nature ~~of the personal data and the nature~~, scope, context and ~~purposes~~purpose(s) of processing~~,~~ and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission ~~and anonymisation or pseudonymisation where this does not prevent fulfilling~~, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this ~~obligation~~paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II ~~[*Technical and organisational measures*]~~. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

7. GDPR Statutory Benefits of Pseudonymisation.

The term Pseudonymisation is used fifteen times in the GDPR, compared to encryption, which is used only four times, and anonymisation which is used only three times. No other Privacy Enhancing Techniques (PETs) are referenced in the GDPR. Statutory benefits granted by the GDPR when implementing compliant Pseudonymisation include, but are not limited to, the following:[49]

- Tipping the balance in favour of Legitimate Interests processing (Articles 5(1)(a), 6(1)(f), and WP29 WP 217)
- More flexible change of purpose (Article 5(1)(b), WP29 WP 203)
- More expansive data minimisation (Articles 5(1)(c), 89(1))
- More flexible storage limitation (Articles 5(1)(e), 89(1))

[49] See www.pseudonymisation.com, www.anonos.com/gdpr-pseudonymisation-benefits and www.dataembassy.com

- Enhanced security (Articles 5(1)(f), 32)
- More expansive further processing (Article 6(4), WP29 WP 217)
- More flexible profiling (WP29 WP 251 rev.01 - Annex 1, Recital 71, Article 22)
- Ability to lawfully and ethically share, combine and enhance data (recitals 42 and 43, Articles 11(2), 12(2), WP29 WP259 rev.01).

D. Three Schrems II Use Cases for GDPR Pseudonymisation

(i) *Expanded Flexibility for Derogations:* Pseudonymisation helps to enable lawful processing if organisations establish as a default the processing of Pseudonymised data whenever, wherever, and as often as possible (as required by GDPR Articles 25 and 32) so that non-Pseudonymised (i.e., identifying) data is processed only when necessary (helping to satisfy GDPR Articles 5(1)(b) Purpose Limitation and 5(1)(c) Data Minimisation), provided that:

- There is a legal basis to do so under Article 6 (e.g., based on Article 6(1)(a) consent, 6(1)(b) contract, or 6(1)(f) legitimate interests by leveraging Pseudonymisation-enabled technical and organisational measures to satisfy the "balancing of interests" test[50]); and
- The processing satisfies derogation requirements (e.g., Article 49(1)(a) based on consent, Articles 49(1)(b) or (c) based on contract).

(ii) *Intra-EEA Processing Obligations*: Pseudonymisation facilitates compliance with GDPR Article 25 and 32 obligations as well as Articles 5(1)(b) Purpose Limitation, 5(1)(c) Data Minimisation, and 6(1)(f) legitimate interests processing (by leveraging Pseudonymisation-enabled technical and organisational measures to satisfy the "balancing of interests" test[51]).

(iii) *Preference for Non-Algorithmically Derived Pseudonyms*: The use of lookup table-based pseudonyms[52] helps to overcome the risk of brute-force unauthorised reidentification by dynamically substituting uncorrelated random Pseudonyms for original data.

A fundamental challenge for all cryptographic methods of data security and protection is that they encode the original information so with sufficient “brute force” processing or quantum computing capabilities, data subjects are, at some level, re-identifiable from the encoded data. Lookup-based pseudonyms make use of random uncorrelated tokens for pseudonymising data, meaning that pseudonyms are not reversible using cryptographic means because they are arbitrarily created without encoding the original data. In this manner, the unauthorised reidentification of pseudonyms within and between data sets via the “Mosaic Effect”[53] is

[50] See https://www.anonos.com/legitimate-interest
[51] Id.
[52] See for example, US Patent No. 10,043,035 Systems and Methods for Enhancing Data Protection by Anonosizing Structured and Unstructured Data and Incorporating Machine Learning and Artificial Intelligence in Classical and Quantum Computing Environments (2018) at https://patentimages.storage.googleapis.com/9e/09/4b/42552a0a31ef8d/US10043035.pdf, expanded global patent coverage is in process according to international treaties. See also https://www.anonos.com/patents
[53] See www.mosaiceffect.com/

defeated because different occurrences of the same data are represented by different pseudonyms. There is no relationship among the pseudonyms without access to additional “look up” information kept separately. Pseudonyms are maximally “entropic” and contain no useful a priori information about the data subject or any data pertaining to the data subject from an information theory point of view. Quantum computing is not able to determine original content based on Pseudonyms that contain zero information about underlying content. **As a result, implementations using lookup-based GDPR-compliant pseudonymisation preserve individual privacy while preventing the re-identification of de-identified data, making sustainable lawful data innovation possible even in a quantum computing world**.[54]

[54] Anonos Data Embassy patented implementation of GDPR-compliant Pseudonymisation supports using dynamically generated random uncorrelated tokens for pseudonymising data. This means that Pseudonyms are not reversible using cryptographic means because they are arbitrarily created without encoding the original data.

Bibliography

Scientific literature

Duball, Joseph. 2021. “A Year after ‘Schrems II’ Ruling, Uncertainty Remains.” July 16, 2021. https://iapp.org/news/a/uncertainty-aplenty-a-year-after-schrems-ii-ruling/.

EDPB. 2021. “Coordinated German Investigation of International Data Transfers | European Data Protection Board.” July 13, 2021. https://edpb.europa.eu/news/national-news/2021/coordinated-german-investigation-international-data-transfers_en.

Foster, Susan L. 2021. “EU Data Protection Regulators Adopt Guidance on Personal Data Transfers.” June 23, 2021. https://www.mintz.com/insights-center/viewpoints/2826/2021-06-22-eu-data-protection-regulators-adopt-guidance-personal.

Helkenberg, Ralf. 2020. “Anonos: Embedding Privacy and Trust Into Data Analytics Through Pseudonymisation”. https://www.anonos.com/hubfs/Embedding_Trust_Into_Data_Anonos_IDC_August_2020.pdf?hsLang=en

Jones, Edward. 2021. “AWS vs Azure in 2021 (Comparing the Cloud Computing Giants).” Kinsta. March 25, 2021. https://kinsta.com/blog/aws-vs-azure/

Klovig Skelton, Sebastian. 2020. “Over Half of Firms Intend to Continue US Data Transfers despite Schrems II.” ComputerWeekly.Com. September 23, 2020. https://www.computerweekly.com/news/252489498/Over-half-of-firms-intend-to-continue-US-data-transfers-despite-Schrems-II

Nielsen, Nikolai. 2020. “US Firms Ignoring EU Court Ruling on Data, Schrems Warns.” EUobserver. September 4, 2020. https://euobserver.com/justice/149329.

Sanchez, Julian. 2021. “TikTok, Schrems II, and Cross-Border Data Flows.” Cato Institute. July 6, 2021. https://www.cato.org/blog/tiktok-schrems-ii-cross-border-data-flows.

Schrems II Hub: Every Development in the Saga.” n.d. Global Data Review. Accessed May 26, 2021. https://globaldatareview.com/data-localisation/schrems-ii-hub-every-development-in-the-saga

European Union law

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council; C/2021/3972; OJ L 199, 7.6.2021. https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

Other Documents

EDPB. 2018. “Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679; Adopted on 25 May 2018.” https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

EDPB. 2020. “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; Adopted on 23 July 2020.” https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

EDPB. 2021. “Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data; Version 2.0; Adopted on 18 June 2021.” https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

Feys, Magali and LaFever, Gary. 2020. Memorandum. https://www.dataembassy.com/

“Question and Answer Sheet Intra-Group Data Traffic.” 2021. www.schremsii.com/German-DPA-Questionnaire.

Schmidt, Christopher. 2021. “Redline (Unofficial) of Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data;” https://www.linkedin.com/posts/piracybydesign_redline-edpb-recommendations-012020-ugcPost-6812701015935082496-i6YT/.

Will, Michael. 2021. “Press Release on Coordinated Audit of International Data Transfers; Interstate Monitoring of Corporate Data Protection Supervisory Authorities to Implement the Schrems II Decision of the European Court of Justice. - Unofficial Translation.” www.schremsii.com/Bavarian-DPA-Press-Release.

Case-law

Judgment of the Court of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559

Sitography

https://www.dataembassy.com/

www.anonos.com/legitimate-interest

www.pseudonymisation.com

www.anonos.com/gdpr-pseudonymisation-benefits

www.mosaiceffect.com

www.enisaguidelines.com

www.anonos.com/legitimate-interest

www.anonos.com/anonymisation-under-the-gdpr

www.anonos.com/data-scientist-expert-opinion

www.anonos.com/TenTruths

Schrems_II_LinkedIn_Group

How Can Organisations Lawfully Process Data in the Cloud After Schrems II?

I. **Summary of University Dissertation Highlighting Why Pseudonymisation is Necessary for Schrems II Compliant Cloud and Remote Processing of EU Personal Data** (4 pages)

The GDPR redefines Pseudonymisation, upgrading it from an ineffective anonymisation technique to a state-of-the-art data protection technical control providing better protection and better utility.

II. **Epilogue to Dissertation Reflecting Impact of Final EDPB Schrems II Guidance, Final European Commission Standard Contractual Clauses, and Increased Emphasis on Pseudonymisation** (18 pages)

The EDPB does not recognize encryption by itself as a lawful instrument of protection of data when utilizing cloud services or when having remote access to data stored in an inadequate third country, other than for the purpose of mere backup. Data pseudonymisation (implemented as defined in Use Case 2 and Article 4(5) GDPR), can be considered, among state-of-the-art technical safeguards available, to be the only lawful bridge available for transfers to third-country cloud service providers.

III. [Background] **Original Dissertation: Cross-Border Data Transfers and Data Localisation in The Aftermath of The Schrems II Judgement by Luigi Madaghiele** (62 pages)

The protection of data through effective technical measures could be the best method of protecting data while ensuring their free flow, independently of the regulatory framework of the third State.

Bachelor's Degree in
Comparative, European and International Legal Studies

CROSS-BORDER DATA TRANSFERS AND DATA LOCALIZATION IN THE AFTERMATH OF THE SCHREMS II JUDGEMENT

Supervisor
Professor
Antonino Alì

Graduating student
Luigi Madaghiele

Academic Year 2020/2021

Bachelor's Degree in
Comparative, European and International Legal Studies

CROSS-BORDER DATA TRANSFERS AND DATA LOCALIZATION IN THE AFTERMATH OF THE SCHREMS II JUDGEMENT

Supervisor
Professor
Antonino Alì

Graduating student
Luigi Madaghiele

Data Protection - Right to Privacy - Schrems
Cloud Computing - Data Localization

Academic Year 2020/2021

Index

Introduction

Digital innovation has brought about many changes in our lives and society, introducing new technologies and indispensable appliances. As many other innovations, nonetheless, also the digitalization process disrupted the existing regulatory framework on many levels. In particular, it created a whole new field of law on digital communication and the protection of digitally collected and processed data.

Within this context, cross-border data transfers acquired remarkable significance. The world of cyberspace, meant to be without borders of any kind, clashes with the physical world where borders are present and States are sovereign on their territory. As a consequence, the right to privacy is subject to different interpretations and the rules governing transfers of data of a State's citizens vary depending on the degree of protection from intrusions awarded by the competent regulatory institution.

The 2013 revelations by Edward Snowden exposed the global surveillance programmes carried out by US Intelligence Agencies: their indiscriminate and unrestricted collection of data brought to light an overreach towards their own and third countries' citizens. With the US not ensuring an adequate level of protection to EU citizens' data, the Safe Harbor regime (governing transfers between EU and US at the time) crumbled in the first *Schrems* case before the Court of Justice of the EU ("CJEU; "the Court). From its ashes, the Privacy Shield regime was negotiated, just to be shattered again in July 2020 by the same Court in the *Schrems II* case. This final dissertation aims at a deep understanding of the latter and its implications, in order to grasp the width of the spectrum of solutions that can be provided by the legislator after the annulment of the Privacy Shield.

The first Chapter, built as an historical overview of the legal framework concerning transatlantic data transfers, also provides a study of the fundamental juridical tools for the protection of privacy and data protection in Europe. Afterwards, it looks at the *Schrems* case, the agreement invalidated by it and its relevance in the case-law of the CJEU. The chapter is concluded with a glance at the negotiation process resulting in the Privacy Shield.

In the second Chapter the focus is switched on the sequel of the above mentioned case, the *Schrems II* case, invalidating the new regime but also interpreting the relevant law as requiring undertakings to introduce additional safeguards to protect flowing data in cases in which their own assessment where the receiving State's level of protection is not sufficient. It will also explore the remaining lawful alternatives justifying the transfer and how these are impacted by the requirements of *Schrems II*. The Chapter culminates with an insight on Brexit and its effect on EU-UK data flows.

The third Chapter aims at the comprehension of new trends, both in the technological and regulatory field affecting cross-borders transfers. Respectively the increasing use of cloud storage/computing and the introduction of data localization policies are impactful on data trades and flows, and embody the two visions of the future of data flows: either liberal and trade-friendly or much more restricted and protectionist. Nonetheless, the two views are not as radical and incompatible as they seem: possibly, *in medio stat virtus*.

Chapter 1: History of the regulatory framework of transatlantic data transfers

1.1 Legal bases in the European Union for the right to privacy and the protection, process and transfer of data

Since the entry into force of the Lisbon Treaty, the Charter of Fundamental Rights of the European Union ("CFREU; "the Charter) has the same legal value of the Treaties. This has been a fundamental step for the European Union ("EU), which was coming from the failed attempt to establish a Constitution for Europe. The lack of a binding Charter providing a set of shared fundamental rights among Europeans until 2009 did not imply that those rights were not protected by the Court of Justice of the European Union before; already in 1974, in *Nold*[1], the Court concluded that it had jurisdictions on fundamental rights, basing these powers on the 'general principles of the EU' that can be found in the common constitutional traditions of the Member States and in the Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR; "the Convention). As it may be inferred from this, the CFREU suffered a great influence from the authority of the ECHR in its drafting, being the latter and the case law of the CJEU so coordinated. Nonetheless, the high level of integration of the EU allowed the drafters to explicitly include other rights not envisaged in the Convention: among these, the right to protection of personal data. Article 8 CFREU starts by recognising such a right to data subjects (the individual whose information refer to), and continues establishing that data must be "*processed fairly for specified purposes and on the basis of the consent*" and that everyone has the right of access and to the rectification of their data.

The ECHR, on its side, doesn't include such a provision: yet, the right to data protection has been incorporated through case law under Article 8 ECHR, concerning the right to respect for private and family life, the equivalent of Article 7 CFREU. Nonetheless, within the framework of the Council of Europe, there is a noteworthy international instrument regarding this right: the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, referred to as 'Convention 108'. This treaty, also accessed by non-members of the Council of Europe, has been a pathbreaker, as it set out ground rules for international data transfer and their processing.

The right to privacy is one of the most basic human rights: it is connected to the human need of sheltering, of having a safe space of 'seclusion', excluding others from some (or all) aspects of our lives. It is supposed to pursue final values of liberty, autonomy and self-determination[2], all necessary for the correct development of liberal democracies. Moreover, the European understanding of the right to privacy also focuses on the negative obligation that the State bears

[1]Judgment of the Court of 14 May 1974, *J. Nold, Kohlen- und Baustoffgroßhandlung v Ruhrkohle Aktiengesellschaft*, C-4/73, ECLI:EU:C:1974:51.

[2] Rouvroy, Antoinette, and Poullet, Yves. 2009. "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy." In *Reinventing Data Protection?*, edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt, 45–76. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-1-4020-9498-9_2.

not to intrude on its citizens' private space, unless certain circumstances are in place. The right to protection of personal data, instead, to a certain extent is intertwined with the right to privacy, as the objectives pursued cross in part. It is believed that Article 8 has been introduced in the Charter to pursue two objecitves: the reduction of information and power asymmetries between the data subject and the controller[3] and 'informational self-determination'. These are arguably two aims that the right to privacy, notwithstanding the extensive interpretations it has had, are better protected by Article 8 CFREU.

Power asymmetries are evident in different phases of the journey of personal data: already in the moment in which consent for processing is being provided powers are not balanced, because while corporations, collecting informations, know the possible uses of data and write the 'terms and conditions' themselves, the individual very likely won't be in the position of assessing the possible harms the processing her or his data may give rise to. Moreover, it may be argued that even if an individual is able to realise s/he has suffered a wrong s/he may not be able to identify its perpetrator.

Informational self-determination refers to the control the individual needs to have on the data and informations concerning her/him to live a life that is self-determined[4]. On one hand, it addresses the influence that surveillance potentially has on the life of the individuals, interest that can also be envisaged within the right to privacy; on the other hand, it advances a relatively recent concept, that is the facilitation of 'selective presentation', the capacity of revealing only the information concerning ourselves and our life we want to show to the people we select[5]. A limitation of both these aspects of our lives is not something that can be tackled by a negative obligation towards the rest of the world with regard to our data: such event would not just limit our freedom and autonomy, but it may affect our behaviour up to the point in which the right to personality is compromised.

As previously mentioned, the spheres of application of Articles 7 and 8 of the Charter intersect where the interest to have a personal, private space needs to be protected, either online or in real life. The definition of a positive right to data protection, reinforced by a purpose limitation and a consent clause, better suits the protection of other facets of our life.

The EU took upon itself the burden of providing extensive legislation on the matter, as it was established in Article 16 of the Treaty on the Functioning of the European Union ("TFEU). Together with Article 8, they are the legal basis for the enactment of the General Data Protection Regulation[6] ("GDPR), probably the most extensive and complete set of rules on the matter in history. The GDPR

[3] Lynskey, Orla. 2014. " Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order." *International and Comparative Law Quarterly* 63 (3): 569–97. https://doi.org/10.1017/S0020589314000244.

[4] Rouvroy, Poullet. 2009.

[5] Lynskey, Orla. 2014.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

repealed the previous Data Protection Directive[7] ("DPD), in force during the whole life of the Safe Harbour regime, the framework for the protection of personal data in the transfer between the EU and the USA in force until the first *Schrems* judgement[8] of the CJEU. Article 25 DPD established the procedure for the assessment of the level of protection offered by third countries, with the aim of ultimately providing the third country with a Commission's adequacy decision. Such provision has been substituted by Article 45 GDPR, complemented by other modalities for ensuring that 'the appropriate safeguards' are provided, namely binding corporate rules ("BCRs) and contractual clauses approved by the Commission; the GDPR also provides for the use of codes of conduct and the setting up of a certification mechanism, yet to be implemented and also discussed later.

Overall, the current legal framework of protection of personal data in the EU is extensive and provides sufficient guarantees to the underlying fundamental rights. Nevertheless, its application with regard to the transfer of data to third countries, where the GDPR doesn't apply, may interfere negatively with such protection. The Court of Justice, the Commission, the national Data Protection Authorities ("DPAs) and privacy and data protection NGOs are all important actors in the enforcement phase of this legislative framework.

1.2 The Schrems I judgement. C-362/14

In order to properly understand the recent developments in the regulatory framework of data transfers between the EU and the US, a step back is required. As above mentioned, until the 6th October 2015, transfers relied on adequacy Decision 2000/520[9] ("the Safety Harbour Decision), setting up the 'Safety Harbour Privacy Principles'. The principles of notice, choice, onward transfer, security, data integrity, access, enforcement were all negotiated between the US Department of Commerce ("DoC) and the Commission and were adhered to by companies on a voluntary basis[10]. Adhering firms were required to issue annually a statement of compliance, and the Federal Trade Commission ("FTC) was entrusted with the powers to monitor compliance in the US.

In 2013, the revelations of the whistleblower Edward Snowden on programmes of mass surveillance undertaken by United States' agencies such as the NSA and the CIA raised concerns on data and the impact they may have on society. Programmes like 'PRISM' and 'Tempora' collected data either by

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[8] Judgment of the Court of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650

[9] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce OJ L 215, 25.8.2000

[10] Solove, Daniel. 2015. "Sunken Safe Harbor: 5 Implications of Schrems and US-EU Data Transfer." TeachPrivacy. October 13, 2015. https://teachprivacy.com/sunken-safe-harbor-5-implications-of-schrems-and-us-eu-data-transfer/

asking big internet corporations to surrender such data to the Agencies for purposes of "national security" or by placing data interceptors on fibre-optic cables with the help, voluntary or forced, of the operators of such cable[11]. And what's more, he also exposed the existence of an agreement between the so called "Five Eyes" (Australia, New Zealand, the UK, Canada and the US), through which these countries systematically share all data they're able to gather[12]. All this was the result of the wave of anti-terrorism policies carried out by the US governments after the occurrencies of the 11th of September 2001, and it was very poorly regulated; this will be discussed later on.

A privacy activist and Facebook user, Mr. Schrems, concerned about the lower standard of protection to which his data were subject to, complained to the Irish DPA, the Data Protection Commissioner, being Ireland the place where Facebook is established in the EU. He questioned the lawfulness of the transfer to the US in the light of these revelations, but the DPA at first rejected its claim declaring that they didn't have the competence to do so, as the transfer between Facebook US and Facebook Ireland relied on the Safe Harbour Decision. Schrems asked for a judicial review of such a decision before the High Court of Ireland, which respectively demanded a preliminary ruling to the CJEU asking for clarification on the role of DPAs in cases akin to this and questioning the lawfulness of the Safe Harbour, as they deemed it in contrast to the Irish Constitution and Articles 7 ,8 and 47 CFREU[13] (the latter concerning the right to an effective remedy).

The Court's judgement started from an evaluation of the position of DPAs in such situations. Putting emphasis on the independence of national DPAs and on the effectiveness of the protection of the individuals' rights[14], it recognised them the competence to examine individuals' claims and investigate them, notwithstanding the presence of an adequacy decision issued by the Commission. It continued by stating that all the acts of the EU must be potentially subject to judicial review - principle descending from the *Kadi*[15] case - and that only the CJEU was entrusted with the power to declare a Decision invalid. Therefore, the subject could either see her/his claim accepted by the DPA of the Member State where the claim was lodged and file a complaint before the competent national Court or could have her/his claim rejected and potential access to judicial remedy contesting the refusal[16]. In any case, although the Court of the Member State at stake could reason on the merit of the Decision, only the CJEU could declare its invalidity. DPAs can, therefore, accept claims of individuals even where an adequacy decision has been issued.

---

[11] Shubber, Kadhim. 2013. "A Simple Guide to GCHQ's Internet Surveillance Programme Tempora." *Wired UK*, June 24, 2013. https://www.wired.co.uk/article/gchq-tempora-101.

[12] Greenwald, Glenn. 2014. *Sotto Controllo. Edward Snowden e La Sorveglianza Di Massa,*. First. Rizzoli.

[13] Monteleone, Shara, and Laura Puccio. 2017. "From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU US Data Transfer Rules : In Depth Analysis." Publications Office. https://data.europa.eu/doi/10.2861/09488.

[14] CJEU, C-362/14, *Schrems*, para. 41.

[15] Judgment of the Court of 18 July 2013, *European Commission and Others v Yassin Abdullah Kadi*, C-584/10 P, ECLI:EU:C:2013:518.

[16] CJEU, C-362/14, *Schrems*, para. 60-65.

The reasoning continued by switching the focus on the validity of Decision 2000/520 itself. The Court admitted that "*neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection*"[17]; yet, Article 25 established that the adequacy decision was the consequence of the Commission recognising that a country ensures the required level of protection in the light of its domestic law and international commitments, all this respecting the freedoms of the individuals recognised in the Charter[18]. Building up from this, and following the Advocate General's ("AG) opinion[19], the CJEU settled a principle that is considered today essential in the legal framework for extra-EU transfers of personal data: the requirement for the third country to maintain an 'adequate level of protection', as referred to in Article 25(6), stands in need of a level of protection that is 'essentially equivalent' to the one provided in the EU, in line with Articles 7 and 8 of the Charter. The Court specified that the means the third country uses to enforce protection might not be the same the US provides, although they are required to be effective and subject to a continuous assessment by the Commission[20].

The last part of the judgement pointed at the Decision itself to check its validity. It especially targeted paragraph 4 of Annex I to the Decision, regarding the possible limitations to the applicability of the Safe Harbour principles for reasons of national security, public interest or law enforcement requirements. The existence of this clause confirmed that interferences with fundamental rights of EU citizens, even for the national security reasons of the third State, were not illegal *per se*. Still, even the Commission itself in a Communication of 2013[21] had found that US authorities had been able to have undiscriminated and generalised access to the data of EU citizens too, blatantly overstepping Safe Harbour's purpose limitation principle: the Court declared that this was exceeding the requirements of strict necessity and proportionality in place where a fundamental (not absolute) right is being limited for the sake of a higher purpose[22]. This overreach was also aggravated by the hardship of having administrative or judicial redress, as the FTC is only competent for commercial disputes. The total absence of objective criteria to be applied in the collection and process of data, and even the lack of an aim to be pursued when doing so, led the CJEU to declare Decision 2000/520 invalid. At this point, it was evident that the limitations to fundamental rights were far from being strictly necessary, and the level of protection of data offered by the US according to the Safe Harbour Regime was far from being essentially equivalent to the one of the EU.

---

[17] CJEU, C-362/14, Schrems, para. 70.

[18] CJEU, C-362/14, Schrems, para. 71.

[19] Opinion of Advocate General Bot delivered on 23 September 2015, Maximillian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:627, para. 141.

[20] CJEU, C-362/14, Schrems, para. 73-76.

[21] Communication to the European Parliament and the Council of 27 November 2013, COM(2013) 846 final, 'Rebuilding Trust in EU-US Data Flows'. https://eur-lex.europa.eu/resource.html?uri=cellar:4d874331-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF

[22] CJEU, C-362/14, Schrems, para. 90.

The Schrems case has also been central in the doctrine concerning the 'essence' of fundamental rights. In the whole array of fundamental rights two categories can be distinguished. On one hand there are absolute rights, which limitation would undermine the highest value of human dignity, and on the other there are those fundamental rights which can be limited in the interest of a higher purpose. Limitations of fundamental rights are in fact envisaged under Article 52 CFREU, which wording establishes that these restrictions should "*respect the essence of those rights and freedoms*". From this the expression used in para. 94-95 of the judgement, stating that the EU measure didn't respect the essence of the right to private life and the right to effective legal protection.
It has been noted that the CJEU didn't engage at all in a balance of interests between the right to privacy and the interest of national security of the US, and that this is because the essence of the former had already been compromised up to a point in which the existence of the fundamental right itself is called to question[23]. As Lenaerts, eminent scholar and vice president of the sitting Court in *Schrems*, explains in a paper[24], the proportionality test and the respect-for-the-essence test are different and are governed by the following relation: where the essence of the right in question is compromised by its limitation the proportionality test is superfluous, while if the measure doesn't conflict with the right's essence it doesn't necessarily mean it is lawful, as it can be disproportionate and respectful of the essence at the same time. It must be noted that this has also been an expedient not to enter into the merits of US national security law allowing the massive collection and storage of data and their proportionality with regard to the aim pursued, avoiding what could be considered as an extraterritorial overreach by US authorities.

The issuance of the *Schrems* judgement was seen as the end point of a series of judgements of the CJEU concerning data and privacy. First, *Digital Rights Ireland*[25] in 2014 invalidated the Data Retention Directive[26] because of an extensive metadata retention requirement, deemed disproportionate by the

[23] Brkan, Maja. 2018. "The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core." *European Constitutional Law Review* 14 (2): 332–68. https://doi.org/10.1017/S1574019618000159. The author develops this concept from the consolidated case law developed in the following judgements, concerning other fundamental rights: *Spasic*, C-129/14 PPU; *Alemo-Herron*, C-426/11; *Florescu*, C-258/14.
[24] Lenaerts, Koen. 2019. "Limits on Limitations: The Essence of Fundamental Rights in the EU." *German Law Journal* 20 (6): 779–93. https://doi.org/10.1017/glj.2019.62.
[25] Judgment of the Court of 8 April 2014, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others*, C-293/12, ECLI:EU:C:2014:238.
[26] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

Court[27]. Then, in *Tele2 Sverige*[28] a national measure transposing the Directive on Privacy and Electronic communications[29] was struck down because of its excessive derogations from the protection of the Directive[30]; it condemned general and indiscriminate retention of data and considered it disproportionate for the purpose of fighting serious crimes. Moreover, this case settled the discussion concerning the differences in scope between Articles 7 and 8 CFREU, as it stated clearly that the two rights are distinct[31]. Lastly, in *Schrems* it is clarified that the standard of protection that third countries need to put in place for data transfers from the EU equals the protection of the essence of the fundamental right to protection of personal data[32]. Yet, more than an end point, Schrems is the starting point of a complex journey that would lead to the current state of affairs.

1.3 The transition from the Safe Harbour regime to the Privacy Shield framework

The US and EU markets are remarkably interconnected: in 2015 they were main trade partners in the amount of goods and services traded[33], relationship that is still ongoing notwithstanding the growth of the Chinese economy[34]. The flow of data is essential for carrying out business, as the data transferred from the US to the EU and *vice versa* have the most various nature, dealing with transactions, investments, delivery of services, human resources, etc…[35]. Especially with the constant increase of the use of technologies such as *cloud computing* and *big data*, which rely on the flow of data and their processing in the most economically convenient place, it is crucial to both establish a clear framework allowing data transfer and ensure their protection.

At the point of its invalidation, *circa* 4500 companies relied on the Safe Harbour regime[36]: these were not only web giants, as one may think, but also small and medium enterprises ("SMEs); the latters see in the internet a huge

---

[27] Brkan, Maja. 2019. "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning." *German Law Journal* 20 (6): 864–83. https://doi.org/10.1017/glj.2019.66.

[28] Judgment of the Court of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, C-203/15, ECLI:EU:C:2016:970.

[29] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[30] Pfisterer, Valentin M. 2019. "The Right to Privacy—A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy." German Law Journal 20 (05): 722–33. https://doi.org/10.1017/glj.2019.57.

[31] CJEU, C-203/15, *Tele2 Sverige AB*, para. 129.

[32] Brkan, 2019. "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning.".

[33] Maisse, Odile, Giulio Sabbati, and Laura Bartolini. 2016. "US: Economic Indicators and Trade with the EU".

[34] Sabbati, Giulio. 2018. "US: Economic Indicators and Trade with EU," 2.

[35] Meltzer, Joshua. 2015. "Hearing on 'Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows.'"

[36] Solove, 2015. "Sunken Safe Harbor: 5 Implications of Schrems and US-EU Data Transfer."

opportunity to expand their markets, and don't often have the means that the equivalent multinational offering the same good/service has to understand and implement changes in the regulatory framework. For this reason, and for the purpose of clarity, the Article 29 Working Party issued some guidelines on the implementation of the *Schrems* judgement. Article 29 Working Party, or WP29, has been the predecessor of the European Data Protection Board, and it was a group composed by a member for each DPA of the Member States, a member for each institution of the EU and a member of the Commission; it took the name from Article 29 of the DPD which established it, and it was vested with advisory powers. In its statement, WP29 clarified three fundamental problems individuals were having in the aftermath of the judgement, that were (1) whether transfers performed before the ruling were lawful, (2) if there was a transitional period for firms to adjust, and (3) which were the legal basis for transfers to the US from that moment on.

(1) With regard to the first point the Working Party stated that transfers still taking place under the Safety harbour regime were unlawful. The effect of the judgement was in fact retroactive, annulling the Decision *ex tunc*, meaning that transfers occurring under that regime were never lawful.
(2) Second, they established a transitional period of three months in which the judgement would not be enforced by the DPAs, to give to the companies a margin in which they could adapt their means of giving protection to personal data to the updated framework.
(3) Third, they ensured the validity of other transfer tools, such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs); a third legal instrument included by the WP29 was the provision of an informed consent to the collection and processing of data, that is still bound to be used as a derogation from the other two, and not as a systematic means of protection[37].

Reliance on the Safe Harbour Principles was popular because of its accessibility; SCCs and BCRs, with their strengths and weaknesses, were very often not the preferred instrument. If one wants to set up a system of contractual clauses, s/he needs to set up these clauses in the relation between the controller and the data subject, between the EU and the non-EU controller[38], and between the controller and the processor[39]. Once these clauses are established, the DPA of the Member State authorising the transfer needs to assess them and communicate them to the Commission, which has a right to oppose. The Commission is also empowered to issue a Decision setting out standardised contractual clauses that don't need a case-by-case authorisation ensuring the

[37] Monteleone, Shara, and Laura Puccio. 2017. "From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU US Data Transfer Rules." Publications Office. https://data.europa.eu/doi/10.2861/09488.
[38] According to Article 4(7) GDPR, a 'controller' is "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*;".
[39] According to Article 4(8) GDPR, a 'processor' is "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*;".

appropriate safeguards[40]. Diversely, Binding Corporate Rules are binding rules, adopted by a group of corporations or enterprises, that only apply to transfers of data outside the EEA within the same group. To adopt such rules, the groups needs to set up an audit mechanism and adopt a set of enforceable measures, placing an obligation on the entire company to comply with pre-approved data protection standard[41]. A legal entity needs to be subject to enforcement measures, preferably a member of the corporation set up in Europe; conversely, if no entity is present in the EEA, other mechanisms of liability need to be established.

As it can be inferred from the complexity of the latter means of protection of data, BCRs are too expensive to set up for SMEs, and definitely not appropriate. SCCs, instead, are more affordable, also because of their standardisation; they are sometimes used as a precautionary measure by particularly scrupulous companies, in addition to the principles set out by an adequacy decision, if present. The Commission is today revisiting the SCCs enacted in 2001, 2004 and 2010, replacing them with a single implementing decision[42]. It is important to mention that as a consequence of the *Schrems* ruling both SCCs and BCRs too will need to ensure a level of protection "essentially equivalent" to the one of the EU, to ensure the certainty and uniformity of EU law.

Being the remaining instruments not sufficient to satisfy the entirety of potential transferors to the US for several reasons, the Commission and the US Department of Commerce convened to renegotiate a new agreement to suppiant the invalid Safety Harbour. In the process of the negotiations, the US committed to impose stronger limitations to the collection and access to personal data[43]. WP29, in return, on the 2 February 2016 released a statement highlighting four important points the new agreement should include for it to be in line with the jurisprudence of the time[44]:

(1) Data processing should be based on clear, precise and accessible rules.
(2) Proved necessity and proportionality with regard to the legitimate objectives pursued, that is, national security.
(3) An independent, effective and impartial oversight mechanism (a judge or another independent body).
(4) Effective remedies available to anyone[45].

The first draft of the new agreement, the 'Privacy Shield', coming to the public on 29 February 2016, was not positively welcomed by WP29. Criticisms concerned the opaqueness of the draft, the independence of the Ombudsman (the body the US proposed to introduce to supplement the lack of judicial redress)

[40] Monteleone, Puccio. 2017. "From Safe Harbour to Privacy Shield", page 13.
[41] Mildebrath, Hendrik. 2021. "EU-UK Private-Sector Data Flows after Brexit: Settling on Adequacy." Publications Office. https://data.europa.eu/doi/10.2861/595569.
[42] Draft Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, public consultation, European Commission, 12 November 2020. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries_it
[43] Monteleone, Puccio. 2017. "From Safe Harbour to Privacy Shield", page 16.
[44] *Ibid*.
[45] *Ibid,* page 17.

and the absence of any effort other than commitments with no binding force towards the abolition of bulk collection of data. Arguments were brought that the problem in the US was structural, that the Privacy Shield was just an attempt to put the dust under the carpet and that it was very likely that also the new agreement would have been struck down by the CJEU. These arguments, that would have proved truthful, reached decision-makers through a variety of means; consumer associations, privacy associations and also authoritative scholars reached the Congress advising against the negotiation of a new agreement without a revision of US Privacy law. They were advised to enact the Consumer Privacy Bill of Rights, to modernise the Privacy Act 1974 (regulating the collection and use of data by Federal Agencies), to establish a fully independent data protection agency and to ratify Convention 108, in order to set up a regulatory framework that is in practice "essentially equivalent" to the one of the EU and safeguard transfers to the US with the right means[46]. The Congress disregarded these suggestions, opting for the negotiation of a new agreement, implementing merely the absolute minimum required to allegedly comply with the *Schrems* judgement. On 12 July 2016, the new adequacy decision was adopted by the European Commission, instituting the Privacy Shield regime.

1.4 The Privacy Shield Decision

Notwithstanding the criticisms it received, Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield brought several changes to the principles contained in the former regime. It was followed by a practical guide[47] of the European Commission addressed to individuals, trying to clarify the principal adjustments from the former regime.

First, companies that wanted to self-certify under the new Privacy Shield were obliged to make their privacy policies available to the public and to designate an independent dispute resolution body dealing with the complaints from data subjects.

The principle of choice, originally allowing subjects giving their consent to opt out from their data being transferred to third parties or used for a purpose different to the original, was modified to allow opt outs even in cases in which the purpose is different but still compatible with the original one.

With regard to onward transfers, third parties were allowed to process the data collected by the corporation participating to the Privacy Shield for the original purpose for which data subjects consented to, as long as the third party ensured a level of protection equivalent to the previously mentioned regime; where it had not been possible to comply with these principles anymore, they needed to notify the corporation adhering to the Privacy Shield so that they could take the appropriate steps to avoid infringements of the obligations set out in the Decision.

---

[46] Rotenberg, Marc. 2020. "Schrems II: From Snowden to China: Toward a New Alignment on Transatlantic Data Protection." *European Law Journal* 26 (1–2): 141–52. https://doi.org/10.1111/eulj.12370.

[47] European Commission, 2016. "Guide to the EU-US Privacy Shield". Available at: https://ec.europa.**eu**/info/sites/default/files/2016-08-01-ps-citizens-**guide**_en.pd_.pdf

Concerning access to one's own personal data, it was possible to receive information on who's processing one's personal data in a reasonable time, without providing a justification for the access and only against a non-excessive fee. Restrictions to this right were only allowed for exceptional circumstances or situations in which such limitation is necessary and duly justified.

Also the security requirement was reinforced, demanding the presence of reasonable and appropriate security measures to be assessed taking into account the risk to which data are exposed.

Last but not least, the principle of data integrity was complemented by a purpose limitation clause and a time constraint: data can be retained and processed only for the purpose to which the subject consented to and for the time required to pursue that objective; yet, this section doesn't impose an obligation on the firm to state a specific time limit for the retention of their data in their privacy policies[48].

Together with these requirements, the Decision introduced much more comprehensive enforcement obligations. Redress mechanisms, declared insufficient to satisfy the right to an effective remedy by the CJEU in *Schrems*, were therefore radically improved in the Privacy Shield framework. The avenues for individuals that wanted to bring a claim for a breach of the obligations borne by a company became several and involved different bodies. First of all, companies needed to set up a contact point to which claims could be sent, and a redress mechanism. Complaints of this kind could also be sent to the Department of Commerce, to the competent DPA or to the independent resolution body designated by the organisation; the latter was empowered to issue a decision including sanctions and remedies and, in case the company didn't comply with the decision, individuals could find remedies by complaining to other authorities with competence to investigate unfair and deceptive practices. Another path could be to file a complaint with the competent DPA, if the company accepted to cooperate: the DPA was empowered to deliver an opinion which, if not respected, could be sent by the same authority either to the FTC or the DoC (depending on the competences for the specific case). The FTC could also be appealed to directly by the individuals, although priority would have been given to complaints coming from DPAs. As a last resort, the new regimes instituted the 'Privacy Shield arbitration panel': if the other means weren't able to resolve the complaint, a panel of three judges vested with the powers of awarding non-monetary remedies[49] was set up by the DoC and FTC.

Instead, as far as concerns the provision of remedies for undue access and use of data by US public authorities, the US legal framework completely lacked a functioning redress mechanism for non-US citizens. The root of this problem can be found in the pieces of legislation that allowed surveillance in the first place, Executive Order 12333 and the 1978 Foreign Intelligence Surveillance Act ("FISA). The latter, in its section 702, allows US intelligence agencies to engage in surveillance programmes targeting non-US persons located outside the territory of the United States; it is addressed to "individually identified legitimate targets", but from the Snowden leaks the public is now aware of the falsity of that

[48] Monteleone, Puccio. 2017. "From Safe Harbour to Privacy Shield", pages 22-24.

[49] Ibid, pages 24-27.

claim. It was as a consequence of the 2013 scandal that the US' legislator decided to step in with the 2015 USA Freedom Act, introducing minimisation rules for surveillance under FISA, and the 2014 Presidential Policy Directive 28 ("PPD-28), which limits signal intelligence ("SIGINT) operations for just six specific purposes and focusing on specific targets through the use of discriminants or selecors.

It needs to be mentioned that FISA includes a redress mechanism for non-US citizens that suffered unlawful electronic surveillance by intelligence agencies; yet, because of the high threshold of the standing requirements and because of the classification of the information concerned, claims rarely have reached a positive outcome. The American Courts may also be petitioned under a series of Acts like the 'Computer Fraud and Abuse Act' or the 'Right to Financial Privacy Act', that are still too specific to ensure the right of access. It's because of this context that the Privacy Shield negotiations led to the introduction of the Privacy Shield Ombudsperson, an allegedly independent body that should ensure investigation of individual claims. The Ombudsperson is assisted by the already existing investigation structures, like the Inspectors-General and the Privacy and Civil Liberties Oversight Board ("PCLOB).

The role of the Ombudsperson has been immediately criticised on two fronts. First, the Ombudsperson wasn't able to confirm or deny whether an individual had been subject to surveillance measures; secondly, and most importantly, the Ombudsperson was an Undersecretary of the US State Department. Its independence, therefore, was questionable[50].

In terms of affordability, the new regime was still very accessible, as prices for certification fluctuated between $250 and $3.250, depending on the company's revenue[51]. It has been commented, though, that the implementation of the Privacy Shield implied much more than just paying a fee: an important amount of money and time needed to be spent to implement the policies and procedures introduced by it[52].

The Privacy Shield represented the endorsement of the Commission toward the ways the US accessed and used data, implying that the essence of the right to privacy was not interfered with anymore. They had in fact the chance to make all the due questions to understand how mass surveillance worked and which safeguards were in place with the data, with the possibility of negotiating a higher threshold of protection for EU-US data transfers. Nonetheless, it has been noted that access to the content of these data has not been forbidden in any way: most notably, it is the generalised access that seems to be prohibited more than non-generalised access[53]. Bulk collection of data was not addressed in the new regulation either. What the Commission had been able to receive was just an

[50] Monteleone, Puccio. 2017. "From Safe Harbour to Privacy Shield", page 32.

[51] Cory, Nigel, Daniel Castro, and Ellysse Dick. 2020. "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation." Information Technology and Innovation Foundation. https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic.

[52] Ibid.

[53] Brkan, 2019. "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning.".

assurance that bulk collection would have been exceptional and 'as tailored as feasible'[54].

2. The Schrems II judgement. C-311/18

2.1 The judgement and its innovations

Since the first Schrems decision of the CJEU, many noteworthy occurrences concerning privacy altered the idea society had of the relation between data and privacy. The Cambridge Analytica scandal increased the awareness of the impact that unsupervised collection and processing of personal data can have on the democratic processes and on voting behaviours. Connected to this, both the election of Donald Trump and Brexit had an impact on the geopolitical global connections, particularly in the second case because of the departure from the EU of a State with one of the most developed signal intelligence gathering institution, the Government Communication Headquarter ("GCHQ). Moreover, while the GDPR was enacted and acquired full effectiveness, many european States updated their surveillance laws as a response to the terrorist attacks of 2015[55].

Many of these conditions arose in the development of the second *Schrems* judgement of the CJEU, deriving from the reformulated complaint of the privacy activist in the light of the first judgement of the saga. After the invalidation of the Safety Harbour Decision, indeed, the High Court of Ireland annulled the decision rejecting the complaint of Mr. Schrems, giving him the opportunity to bring a new claim reformulated in light of the CJEU judgement. To do so, he needed to know on what basis Facebook Ireland was transferring data to the US after the Safety Harbour invalidation, and had as an answer that the transfer of data to their central branch was ruled by a an agreement between the two, allegedly offering a sufficient level of protection to the data in the transfer[56].

In his revised complaint, Schrems continued to claim that the US did not ensure an adequate level of protection to the data coming from the EU, challenged the validity of the Privacy Shield decision and requested the halt of the transfer of his data to the US on the basis of the SCC; however, he didn't challenge the validity of any SCC Decision[57]. This time, the Data Protection Commissioner accepted the complaint notwithstanding the presence of an adequacy decision, making Schrems reach the High Court, which referred to the CJEU for a preliminary ruling. While in the first judgement the Court was asked to answer just two questions, in the second preliminary ruling the questions are eleven, and much more complicated.

---

[54] Monteleone, Puccio. 2017. "From Safe Harbour to Privacy Shield", page 29.

[55] Bignami, Francesca. n.d. "Schrems II: The Right to Privacy and the New Illiberalism." *Verfassungsblog* (blog). Accessed May 10, 2021. https://verfassungsblog.de/schrems-ii-the-right-to-privacy-and-the-new-illiberalism/.

[56] Tracol, Xavier. 2020. "'Schrems II': The Return of the Privacy Shield." *Computer Law & Security Review* 39 (November): 105484. https://doi.org/10.1016/j.clsr.2020.105484.

[57] Ibid.

First of all, the Court addresses the material scope of the GDPR, regulating in its Chapter V "*Transfers of personal data to third countries or international organisations*" since its entry into force on the 25 May 2018. Reading Article 2 GDPR in light of the renowned Article 4(2) TFEU, which emphasizes the exclusion of the EU from any responsibility in the field of national security, the Court is able to straightforwardly conclude that the fact that data of european individuals are processed in third States for purpose of protection of their public, defence and State security doesn't exclude the application of the GDPR to transfer between an operator inside the EU and another in such third State[58].

Then, it continues by assessing what is the level of protection required by the GDPR in its Article 46 on "*Transfers subject to appropriate safeguards*", the latter including contractual clauses accepted by the Commission. Article 46 states in its paragraph one that it applies "*in the absence of a decision pursuant to Article 45(3)*", an adequacy decision. The reasoning restates and endorses Recital 108 of the GDPR, affirming that in the absence of an adequacy decision of the Commission appropriate safeguards need to be taken by the controller to compensate for the lack of data protection in a third country. The ultimate aim of doing this, as it could be expectable, would be ensuring a level of protection essentially equivalent from what is guaranteed in the EU[59]. The parameters to assess adequacy in this case would be the same used by the Commission in their adequacy procedure, expressed in Article 45(2)[60]. Following this conclusion, the judgment focuses on a clarification of the corrective power that DPAs are vested with to impose a temporary or definitive limitation on processing[61]: in case, for a transfer protected only by contractual clauses, the transferor and the transferee cannot ensure a level of protection essentially equivalent to the one of the EU DPAs are bound to suspend or prohibit such transfer.

With regard to the SCC Decision at stake[62], although Schrems didn't challenge it, the Court engaged in a reasoning on whether such provision ensures an adequate level of protection. SCCs, for their nature, do not bind the authorities of third countries[63], and the Commission does not need to appraise the degree of protection that third countries ensure before allowing the use of SCCs for transfer to these[64]; such effort would be out of the scope the legislator envisaged for the use of contractual clauses, being a way of protecting personal data uniformly outside the EU. With this in mind, the Court determines that controllers and processors must engage, before the transfer and on a case-by-case basis, in an assessment of whether the third country ensures adequate protection[65]. If the third State manages to do so, no additional safeguards are required; on the contrary, "*[i]n so far as those standard data protection clauses cannot [...] provide*

[58] CJEU, C-311/18, Schrems II, para. 89.
[59] CJEU, C-311/18, Schrems II, para. 95-96.
[60] CJEU, C-311/18, Schrems II, para. 104-105.
[61] CJEU, C-311/18, Schrems II, para. 121.
[62] 2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. *OJ L 39, 12.2.2010.*
[63] CJEU, C-311/18, Schrems II, para. 125.
[64] CJEU, C-311/18, Schrems II, para. 130.
[65] CJEU, C-311/18, Schrems II, para. 134.

guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third countries, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection."[66]. It also specifies that the validity of standard clauses depends on whether such clauses are effective in ensuring an adequate level of protection, their effectiveness arising from the 'supplementary measures' included in the agreement. Any alteration to the third State, being it legislative or of any other nature, that is capable of altering the frame of the transfer should be notified to the EU controller of processor, which is asked to notify the competent DPA that will take appropriate measures[67]. Nonetheless, the SSC Decision doesn't affect the autonomous power of DPAs to suspend or prohibit transfers to third countries based on SCCs as appropriate[68].

The CJEU only deals with the elephant in the room, the question on validity of Privacy Shield, at the end of the judgement. Together with Schrems's claim of its invalidity, indeed, also the referring Court brought arguments in favour of its abolition, analysing the legislative context to the US and suggesting the lack of sufficient guarantees. The Court gives an understanding of the relevant EU legislation beforehand, to proceed in a second moment to analyse one by one US pieces of legislation allowing surveillance programmes: the effort of entering into the merits of US regulation, avoided in the first *Schrems* case, is in this case deemed necessary.

First of all, it considers adequacy Decision 2016/1250, which in its paragraph 1.5 of Annex II provides a derogation from its principles to meet national security, public interest or law enforcement rules of the United States[69]. Then, it recapitulates all the human rights at stake, namely Article 7 and 8 CFREU, recalling that these are potentially limitable to meet other objectives of general interest under Article 52 CFREU[70]; this same Article provides that such limitations are subject to an assessment of proportionality, that the Court adjusts according to its previous case law. Quoting *Opinion 1/15 (EU-Canada PNR Agreement)*[71], another landmark decision in this area that followed *Digital Rights Ireland* and *Tele2*, the CJEU establishes that interferences with fundamental rights must have a legal basis which "*must itself define the scope of the limitation*"[72] and must apply just "*in so far as strictly necessary*"[73] to satisfy the proportionality requirement of Article 52.

Only after having set up the previous test, the Court applies it to US legislation. Section 702 FISA, the main legal basis for surveillance carried out by intelligence agencies, provides to some extent supervision by the Foreign Intelligence Surveillance Court ("FISC). Nonetheless, the latter only gives an

[66] CJEU, C-311/18, Schrems II, para. 133.
[67] CJEU, C-311/18, Schrems II, para. 145.
[68] CJEU, C-311/18, Schrems II, para. 146.
[69] CJEU, C-311/18, Schrems II, para. 164.
[70] CJEU, C-311/18, Schrems II, para. 171-172.
[71] Opinion of the Court of 26 July 2017, *Accord PNR UE-Canada*, Avis 1/15, ECLI:EU:C:2016:656
[72] CJEU, C-311/18, Schrems II, para. 175.
[73] CJEU, C-311/18, Schrems II, para. 176.

annual *ex ante* authorisation to pursue mass surveillance[74], definitely not having an 'as tailored as feasible' approach. As a consequence, the level of protection guaranteed by this section is not by any means essentially equivalent to the one of the EU. Together with this provision, also PPD-28 and E.O. 1233 do not satisfy the proportionality test as previously defined by the Court.

The Court also finds that all these measures do not confer actionable rights against US authorities to individuals[75]. As seen before in *Schrems*, the right to a trial and effective judicial protection is fundamental to ensure adequate protection to individuals, and is laid down in Article 47 CFREU. The Ombudsperson mechanism either, despite being regarded by the Commission as providing an adequate level of protection, failed to meet the requirement of independence[76], essential for ensuring fairness in a trial. The Ombudsperson in fact is appointed by and reports to the Secretary of State, expressing executive power.

To conclude, the Court declared the Privacy Shield Decision 2016/1250 invalid, as it failed to ensure a framework of protection of personal data essentially equivalent to the one of the European Union, violating Articles 7, 8 and 47 of the Charter. US surveillance programmes, in fact, are not limited to what is strictly necessary and are disproportionate with regard to the above mentioned rights.

In brief, this judgement introduces two important principles that have various practical implications. First, it establishes the invalidity of the Privacy Shield, finding it in breach of the relevant fundamental rights notwithstanding the updates that it introduced; these were meant to fill in the *lacunae* of the Safety Harbour, but failed. It is important to notice that similarly to *Schrems* also invalidity of Decision 2016/1250 takes effect *ex tunc*[77], while differently from it no grace period was awarded by the EDPB[78]. Secondly, it formulates a principle with which many companies will need to cope with: also those who seek to transfer data pursuant to SCCs, need to ensure a level of protection essentially equivalent to the one of the EU, if necessary by providing 'supplementary measures' to compensate for the lower threshold of the safeguards of the third state; if the operators and processors can't do so, they need to suspend transfers[79].

The Court left the definition of 'supplementary measures', which raised many questions, to the EPDB. Indeed, on 10 November 2020, the latter adopted the "*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*"[80]. The Recommendations describe practical situations companies may find themselves in and suggest potential solutions to ensure the required degree of protection. Annex II to this document, in particular, provides a non-exhaustive list of what supplementary measures may entail, dividing these in three groups: technical

[74] CJEU, C-311/18, Schrems II, para. 179.
[75] CJEU, C-311/18, Schrems II, para. 192.
[76] CJEU, C-311/18, Schrems II, para. 195-197.
[77] Tracol, 2020. "'Schrems II': The Return of the Privacy Shield."
[78] Cory, Castro, Dick, 2020. "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation."
[79] Mildebrath, Hendrik. 2020. "The CJEU Judgment in the Schrems II Case." European Parliamentary Research Service.
[80] Recommendations 01/2020 of the European Data Protection Board adopted on 10 November 2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

measures, additional contractual measures and organisational measures. Effective technical measures for the EDPB can be encryption, pseudonymisation or split processing, although their effectiveness depends on the circumstances. Contractual measures for their nature do not bind the third country authorities, neither can they exclude the application of foreign laws requiring data importers to comply with the authorities' orders: transparency requirements, commitments on the importers to review the legality of the orders they receive, obligations on companies to recognise rights to the data subjects concerned, are all clauses that may contribute to the correct enforcement of the judgement. Lastly, organisational measures have different configurations and go from data minimisation to the adoption of internal policies aimed at the correct application of EU data protection principles.

The fact that a company follows one or more of these guidelines, however, does not downplay the role of the case-by-case assessment of the framework of the third State preceding an evaluation of the most suitable measures, as emphasized in the Court's decision. After this judgement, SSCs will not be treated as simply a formalistic requirement anymore, but as a fully-fledged agreement to be modelled according to the present conditions[81].

2.2 Legal bases for data transfers in the aftermath of Schrems II and their implementation

While the invalidation of the Privacy Shield was somehow expected by the critics, the strengthening of contractual clauses was not. The judgement has been criticised, indeed, for the burden it imposes on the companies to make an assessment of the normative framework of surveillance law of third countries. It particularly affects SMEs, which are likely not to be able to afford such onus and, consequently, will find harder to benefit from innovations that rely on data transfers[82]. Companies who want to transfer data to third countries where law enforcement and security legislation may be difficult to obtain or non-existent may be hampered as well[83], although for different reasons.

The EDPB, as seen above, has issued some instructions to guide organisations toward compliance. In Recommendations 01/2020 on measures that supplement transfer tools[84] they envisage six steps that, if followed, may ensure conformity:

---

[81] Oldani, Isabella. 2020. "The future of data transfer rules in the aftermath of Schrems II." *SIDIBlog* (blog). October 23, 2020. http://www.sidiblog.org/2020/10/23/the-future-of-data-transfer-rules-in-the-aftermath-of-schrems-ii/.

[82] Cory, Castro, Dick, 2020. "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation."

[83] Chander, Anupam. 2020. "Is Data Localization a Solution for Schrems II?" SSRN Scholarly Paper ID 3662626. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3662626.

[84] Recommendations 01/2020 of the European Data Protection Board adopted on 10 November 2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

(1) *Know your transfers*: mapping all the transfers of personal data to third countries and verifying that restrictions imposed by the GDPR, like purpose limitation, apply.
(2) Verify the transfer tool your transfer relies on: recognise on which basis, according to Article 45, 46, or even 49 GDPR in exceptional cases, the transfer is allowed to occur.
(3) *Assess the law or practice of the third country*: the EDPB is reiterating the importance of the transfer impact assessment introduced by the Court.
(4) *Identify and adopt supplementary measures*: only necessary if the third step diagnoses a threat.
(5) *Take formal procedural steps to adopt such measures*: sometimes, in order to add supplementary measures, competent DPAs need to be involved.
(6) *Re-evaluate and monitor at appropriate intervals*: developments in foreign legislation may require a change in the measures previously implemented.

Overall, the EDPB is asking organisations not to process data carelessly and to be conscious of their transfers and how these are protected from interferences, in order to be compliant with the judgement and to avoid fines up to €20 millions or the 4% of their global turnover, as enshrined in Article 83(5)(c) GDPR[85].

Being aware of all the complications that *Schrems II* introduces, the interested undertakings did not take it positively. Notwithstanding Schrems' suggestion to follow the judgement literally, review their transfers and stop the unlawful ones[86], a majority of companies both established in the US[87] and in the EU[88] expressed an intention not to comply with the judgement. Among these it was possible to find Microsoft and Amazon Web Services[89], the main cloud computing services providers in the world[90].

A partner of the company that issued the survey has noted how, instead, businesses that want to be compliant will address the changes in the framework of data transfers: many will just skip the transfer impact assessment, and will only assume that any State they plan to send the data to will simply not provide equivalent protections to the EU. The required case-by-case assessment is not

[85] Mildebrath, Hendrik. 2020. "The CJEU Judgment in the Schrems II Case." European Parliamentary Research Service.
[86] NOYB. 2020. "Next Steps for EU Companies & FAQs." Noyb.Eu. July 20, 2020. https://noyb.eu/en/next-steps-eu-companies-faqs.
[87] Nielsen, Nikolai. 2020. "US Firms Ignoring EU Court Ruling on Data, Schrems Warns." EUobserver. September 4, 2020. https://euobserver.com/justice/149329.
[88] Klovig Skelton, Sebastian. 2020. "Over Half of Firms Intend to Continue US Data Transfers despite Schrems II." ComputerWeekly.Com. September 23, 2020. https://www.computerweekly.com/news/252489498/Over-half-of-firms-intend-to-continue-US-data-transfers-despite-Schrems-II.
[89] "Schrems II Hub: Every Development in the Saga." n.d. Global Data Review. Accessed May 26, 2021. https://globaldatareview.com/data-localization/schrems-ii-hub-every-development-in-the-saga.
[90] Jones, Edward. 2021. "AWS vs Azure in 2021 (Comparing the Cloud Computing Giants)." Kinsta. March 25, 2021. https://kinsta.com/blog/aws-vs-azure/.

necessary if the threshold allowing the transfer is set always at the same level, that is, a level equivalent to the EU[91].

Schrems' NGO 'None Of Your Business' ("NOYB) contacted a set of companies to ask how they were coping with the judgement and which additional safeguards they were planning to put into effect. NOYB either received no answer at all or were redirected to privacy policies, which didn't answer their questions; only Microsoft and few others firms responded properly[92]. The same organisation, after one month from the judgement, filed 101 complaints in 30 EEA States against companies that forwarded data about their visitors to Google and Facebook overseas[93]. These multidirectional actions were brought on the same day to trigger the enforcement of the judgement, contrasting the trend not to comply with the ruling; also in this case, only few organisations responded to the claims. A positive acknowledgment came from the EDPB though, which set up a task force to deal with this load of complaints in a coordinated way[94].

It has been noted that under Article 45 GDPR the responsibility to assess the adequacy of the country of import is borne by the Commission, and that with this new framework SCCs themselves will become 'mini adequacy decisions'[95]. While this may be a good point to reflect on the burden imposed onto companies, it is also true that these contractual clauses are supervised by the national DPA or the Commission itself, which have the last word, dismissing this claim.

Leaving aside the issue of SCCs, the *Schrems II* judgement left those who relied on the adequacy decision without a legal basis for transfer for a second time, and with a different framework to be complied with. As previously mentioned, other modalities of transfers are enshrined in the GDPR, some of which have been indirectly affected by the judgement. The setting up of Binding Corporate Rules, for instance, has been modified to the same extent of SCCs, requiring a case-by-case assessment and the potential adoption of additional safeguards as seen before; this has been expressed by the EDPB in the FAQs following the judgement[96]. Therefore, BCRs do not enjoy a better position

[91] Klovig Skelton, 2020. "Over Half of Firms Intend to Continue US Data Transfers despite Schrems II.".

[92] NOYB. 2020. "Opening Pandora's Box: Companies Can't Say How They Comply with CJEU Ruling." Noyb.Eu. September 25, 2020. https://noyb.eu/en/companies-cant-say-how-they-comply-cjeu-ruling.

[93] NOYB. 2020. "101 Complaints on EU-US Transfers Filed." Noyb.Eu. August 17, 2020. https://noyb.eu/en/101-complaints-eu-us-transfers-filed.

[94] NOYB. 2020. "Update on Noyb's 101 Complaints on EU-US Data Transfers." Noyb.Eu. September 22, 2020. https://noyb.eu/en/update-noybs-101-complaints-eu-us-data-transfers.

[95] Kuner, Christopher. 2020. "The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation." *European Law Blog* (blog). July 17, 2020. https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/.

[96] Frequently Asked Questions of the European Data Protection Board of 23 July 2020 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

compared to SCCs[97] and possibly risk to be more burdensome, as they are more costly[98] and take *circa* two years to be approved[99].

Other guidelines of the EDPB[100], in addition, totally exclude the application of the derogations provided for in Article 49(1)(a) GDPR, allowing transfers in cases in which the individual gave her/his explicit consent. Not only the requirement of an informed consent is difficult to satisfy, but being this a derogation it has been argued that it legitimises only occasional transfers, and can't be used on a systematic basis.

As previously mentioned, the GDPR includes some basis for transfers still to be implemented: codes of conducts and certification mechanisms, both covered by Article 46 GDPR.

In the case of codes of conduct, organisations need to commit to it through a binding agreement, enforced by an accredited independent body[101]. These have a scope larger than BCRs, as they don't apply just to intra-group transfers (although they are developed in a sector specific manner) and once they are accepted by the Commission they can be adhered to by anyone, allowing the accession of less prosperous companies[102]. When they are aimed at the transfer to third countries, they are referred to as 'transnational codes of conduct'. Codes can be drafted either by the Commission itself or by independents, and some are already pending for approval[103]. The EDPB recently issued two positive opinions on the first two transnational codes under the GDPR: the '*EU Data Protection Code of Conduct for Cloud Service Providers*', submitted by Scope Europe, and the *'Code of Conduct for Cloud Infrastructure Service Providers*', submitted by Cloud Infrastructure Service Providers (CISPE)[104]. The procedure could end up with a Commission's implementing act, which could make them effective in all the EU[105].

On the other hand, certification mechanism aim at the issuance of a certificate demonstrating that an organisation is compliant with the GDPR; they are not available to businesses, although the certification procedures have been

---

[97] Tracol, 2020. "'Schrems II': The Return of the Privacy Shield."

[98] Mildebrath, 2021. "EU-UK Private-Sector Data Flows after Brexit"

[99] Cory, Castro, Dick, 2020. "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation."

[100] Guidelines 2/2018 of the European Data Protection Board of 25 May 2018 on derogations of Article 49 under Regulation 2016/679.

[101] *See* Article 41 GDPR.

[102] Mildebrath, 2021. "EU-UK Private-Sector Data Flows after Brexit"

[103] "Complementing the EU Cloud CoC to Become a Safeguard Pursuant Art. 46 GDPR." n.d. EU Cloud Coc. Accessed May 26, 2021. https://eucoc.cloud/en/about/third-country-transfer-initiative/.

[104] European Data Protection Board. 2021. "Transnational Codes of Conduct: Ensuring Consistency and Data Subject Rights through Co-Regulation." Linkedin. May 21, 2021. https://www.linkedin.com/pulse/transnational-codes-conduct-ensuring-consistency-data-subject-/?trackingId=BeDi8wHH9bQpX53YngJLsg%3D%3D.

[105] Étienne Armingaud, Claude. n.d. "EU Data Protection: In a Post-Privacy Shield, Sectorial Code of Conduct Could Lead the Way to Safeguard Data Transfers Outside the EU/EEA." K&L Gates. Accessed May 26, 2021. https://www.klgates.com/eu-data-protection-in-a-post-privacy-shield-sectorial-code-of-conduct-could-lead-the-way-to-safeguard-data-transfers-outside-the-eueea-07-17-2020.

laid down in the GDPR[106]. The practical effect of certification would be loosening up the burden of proof for compliance and serving as an attenuating factor in the case of fines. It has been observed that, differently from other EU certifications, this kind of certification would not necessarily imply that an organisation is GDPR compliant, but it would just show its commitment to the protection of personal data and improve accountability[107]. For its cost, even this option could be unfavourable to SMEs[108].

In both the latter cases, the key concept coming from *Schrems II* of compensatory measures being introduced in absence of an adequacy decision to ensure the protection of data in their transfer and while in the third country remains unvaried. The setting up of these measures would not therefore lower the threshold of protection, but would just standardise mechanisms to improve the accessibility to compliance and facilitate supervision.

It is not a case that so far the negotiation of a new EU-US agreement hasn't been seriously contemplated among the possible future legal basis. Notwithstanding the call for action by stakeholders[109], which still were sceptical of a 'quick fix' approach similar to the negotiation of the Privacy Shield[110], the future existence of a new adequacy decision itself has been doubted for the time being. A joint statement of the DoC and the Commission, declaring the initiation of discussions on a new framework, had been released some weeks after the judgement[111]: at the moment of writing, the US is finalising the proposal that will be set forth in the EU-US summit taking place on 15 June 2021[112]. Still, it can be said that a political agreement is far from being concluded, also because of pessimistic statements from EU officials. Commission's Vice President Jourová[113], the EDPB[114] and Mr. Schrems himself called for a reform in the US

---

[106] *See* Article 42 GDPR.

[107] Kamara, Irene. 2020. "4 GDPR-Certification Myths Dispelled." January 28, 2020. https://iapp.org/news/a/four-gdpr-certification-myths-dispelled/.

[108] Mildebrath, 2021. "EU-UK Private-Sector Data Flows after Brexit".

[109] Digital Europe. 2020. "An Early Analysis of Schrems II – Key Questions and Possible Ways Forward." https://www.digitaleurope.org/wp/wp-content/uploads/2020/08/DIGITALEUROPE_An-early-analysis-of-Schrems-II_Key-questions-and-possible-ways-forward.pdf.

[110] Kristakis, Theodore. 2020. "After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe." *European Law Blog* (blog). July 21, 2020. https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/.

[111] Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross, 10 August 2020. https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en

[112] Scott, Mark. 2021. "Biden Seeks High-Level Data Deal to Repair EU-US Digital Ties – POLITICO." June 2, 2021. https://www-politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/joe-biden-data-transfers-privacy-shield-eu-transatlantic/amp/.

[113] *Ibid*.

[114] European Data Protection Board. 2020. "EDPS Statement Following the Court of Justice Ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ('Schrems II')." July 17, 2020. https://edps.europa.eu/press-publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling_en.

surveillance legal regime[115], being it the ultimate cause of the threat: the answer of a US official has been negative, defining the change in the short term of surveillance laws neither "*advisable nor possible*"[116]. Ironically, the only development in US regulation on the matter is the Protecting Americans' Data From Foreign Surveillance Act (amending the Export Control Reform Act of 2018[117]) which draft has been published in April 2021: the Act aims at stopping transfers of US citizens' personal data to locations with inadequate data protection - just as the GDPR[118]. Albeit the main target of the Bill is probably China, Ireland has been included within the scope of the countries with faulty data protection[119]. Ireland in fact had been regarded as lacking enforcement of the GDPR[120], a situation that Mr. Schrems defined as 'kafkaesque'[121]. Such consideration needs to be seriously addressed, to avoid the hypocrisy of having a GDPR with a 'long arm provision'[122] (applying to processors located in third countries that process data in the context of offering service to the EU) and having Member States of the EU themselves not enforcing correctly the same provision. Moreover, another question arises in this context: would every Member State successfully withstand a test similar to the one carried out by the Commission to ultimately issue an adequacy decision? In other words, do EU surveillance laws adequately protect third countries citizens' personal data?

In the end, in practice, the data flow between the EU and US never stopped, and it's very likely it won't in the future: the show must go on[123]. While an adequacy decision is far from being issued, other instruments are being explored. The breaking off of the Privacy Shield has opened a debate on data sovereignty and data protection. Stakeholders are many and different, as the factors that should be considered. Undertakings primarily need certainty of the rules and

---

[115] NOYB. 2020. "CJEU Invalidates 'Privacy Shield' in US Surveillance Case. SCCs Cannot Be Used by Facebook and Similar Companies." Noyb.Eu. July 16, 2020. https://noyb.eu/en/cjeu.

[116] Manancourt, Vincent. n.d. "EU's Rejection of US Surveillance Also Tests Its Commitment to Privacy." Politico. Accessed May 26, 2021. https://www.politico.eu/article/rejection-of-us-surveillance-tests-eu-mettle-on-privacy-shield/.

[117] Congress.gov. "Text - H.R.5040 - 115th Congress (2017-2018): Export Control Reform Act of 2018." aprile 17, 2018. https://www.congress.gov/bill/115th-congress/house-bill/5040/text.

[118] Moody, Glyn. 2021. "Irony Alert: US Could Block Personal Data Transfers To Ireland, European Home Of Digital Giants, Because GDPR Is Not Being Enfor." *The New York Press News Agency* (blog). April 23, 2021. https://nypress.co.uk/2021/04/23/irony-alert-us-could-block-personal-data-transfers-to-ireland-european-home-of-digital-giants-because-gdpr-is-not-being-enforced-properly/.

[119] Scally, Derek. 2021. "US Senate to Debate Limiting Foreign States' Access to Citizens' Data." *The Irish Times*, April 15, 2021. file:///Users/luigimadaghiele/Zotero/storage/9XF7L9QU/us-senate-to-debate-limiting-foreign-states-access-to-citizens-data-1.html.

[120] Ryan, Johnny. 2021. "New Economic Risk: Draft US Senate Bill and Ireland's GDPR Enforcement." Irish Council for Civil Liberties. https://www.iccl.ie/news/new-us-senate-bill-may-stop-ireland-processing-us-data-unless-ireland-acts-on-gdpr-enforcement/.

[121] Scally, Derek. 2021. "Irish Approach to Data Protection 'Kafkaesque', Says Schrems." The Irish Times. April 9, 2021. https://www.irishtimes.com/business/technology/irish-approach-to-data-protection-kafkaesque-says-schrems-1.4533257.

[122] *See* Article 3(2) GDPR.

[123] Tene, Omer. 2020. "The Show Must Go On." July 17, 2020. https://iapp.org/news/a/the-show-must-go-on/.

procedures to be followed, to avoid the risk of fines (the absence of a grace period didn't favour their interest). Data subjects, represented by privacy organisations, demand a higher international level of protection of their data and the necessary guarantees and remedies to protect from unlawful interferences with their rights. The governments and their agencies need to ensure law enforcement and public and national security; yet, it could be argued that mass collection of any data available is disproportionate to the objective pursued and a waste of resources, as well as infringing fundamental rights. Although the debate on the topic can overall be considered positive, conclusions cannot be drawn for the time being.

2.3 Transfers to post-Brexit UK and third countries

The unprecedented exit of the United Kingdom ("UK) from the EU impacted many aspects of the relation between the two entities: whereas trade is probably the most affected element, many others aspect were influenced, among which data protection and the Area of Freedom, Security and Justice[124]. Leaving aside the long political debate on whether the UK's government would have or would have not concluded a deal with the EU to regulate post-Brexit relations, eventually a long and complex agreement, the Trade and Cooperation Agreement ("TCA), was concluded on the 24 December 2020. It set up rules on many issues, among which trade, travel, provision of services, fishing, security and data protection. Concerning the last two, the UK will no longer have automatic access to key security databases, won't be part of Europol anymore, and will not be obliged to comply with EU standards of data protection any longer[125]. Or will they?

During negotiations, the UK proposed to commit to the free flow of data in advance, basically not to be treated as a third country, with the strong opposition of the EU which relied on its GDPR principles[126]. The openness of the UK to lighter standards of data protection can be inferred from the UK-Japan agreement on trade, which tilts towards the Asia-Pacific data protection regulatory model[127]. The TCA introduced an interim solution or, as it has been defined, a 'bridging mechanism', ensuring the provisional continuation of personal data flows and meant to pave the way to an adequacy decision. This temporary measure[128], initially lasting four months and then extended until 30 June 2021, establishes that for the sake of transfers of data the UK is not considered as a third country until the aforesaid deadline. Still, this clause is subject to several restrictions. First, the UK must not disapply or lower the level of protection provided by its data

[124] *See* Title V TFEU.
[125] Edgington, Tom. 2020. "Brexit: What Are the Key Points of the Deal?" *BBC News*, December 30, 2020, sec. UK. https://www.bbc.com/news/explainers-55180293.
[126] Mildebrath, 2021. "EU-UK Private-Sector Data Flows after Brexit".
[127] Ruiz, Javier. 2020. "Briefing: How the UK-Japan Trade Deal Severs Post-Brexit Data Adequacy." Open Rights Group. November 5, 2020. https://www.openrightsgroup.org/publications/what-the-uk-japan-trade-deal-means-for-digital-rights/.
[128] *See* Article FINPROV.10A TCA.

protection law, namely the UK GDPR and the Data Protection Act 2018 ("DPA 2018). Secondly, the UK is bound not to exercise powers that have the effect of not ensuring the EU level of protection (finding third countries adequate, approving SCCs and BCRs, etc…), unless this exercise is functional to the alignment to EU laws or is authorised by the EU-UK Partnership Council[129].

Civil society organisations expressed their concern about this interim measure, arguing that the UK already at the time of signature was not ensuring adequate protection[130], basing their claim on, *inter alia*, the case law of the European Court of Human Rights ("ECtHR). It is a matter of fact that the ECtHR in September 2018 decided in *Big Brothers Watch*[131] that Britain's 2000 Regulation of Investigatory Powers Act ("RIPA), by allowing bulk data collection without the appropriate restrictions, violated the right to privacy afforded by Article 8 ECHR and, interestingly enough, the right of freedom of expression enshrined in Article 10 ECHR[132]. According to the critics, this 'bridge' model could set up a risky precedent of transfers being lawfully carried out notwithstanding the lack of adequate protection. The EDPS addressed the concern in the *Opinion on the conclusion of the EU and UK trade agreement*[133] stressing that "*such mechanism should remain exceptional and should not set a precedent for future TCAs with other third countries*", reassuring the public.

The UK has a lot to lose from being inadequate, with the exact cost being estimated between €1.116-1.786 billions for UK firms and originating from the cost of setting up mitigating strategies like SCCs[134]. As previously mentioned, an adequacy decision would radically lower these costs, making transfers almost as easy as intra-EU ones[135]. Negotiations on a UK adequacy decision began on 11 March 2020, even before the ratification of the TCA. Only on 19 February 2021 the Commission published two draft adequacy decisions, one of which governing exclusively private data flows, maintaining that the UK ensures standards of data protection essentially equivalent to the EU. This has been also endorsed by field

[129] Church, Peter, and Georgina Kon. n.d. "Brexit: Where Does the Adequacy 'Bridge' Lead To?" Linklaters. Accessed May 28, 2021. https://www.linklaters.com/en/insights/blogs/digilinks/2021/january/brexit---where-does-the-adequacy-bridge-lead-to.

[130] Massé, Estelle. 2021. "Access Now's Memo on the Data Transfers and PNR Provisions under the EU-UK Trade Agreement." AccessNow. https://www.accessnow.org/cms/assets/uploads/2021/01/EU-UK-Deal-Data-transfers-PNR.pdf.

[131] Big Brother Watch and others v. United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15) [2018] ECHR 722.

[132] O'Donoghue, Cyinthia, and Nona Keyhani. 2018. "ECtHR Rules on UK Mass Surveillance under RIPA." Technology Law Dispatch. October 25, 2018. https://www.technologylawdispatch.com/2018/10/in-the-courts/ecthr-rules-on-uk-mass-surveillance-under-ripa/.

[133] Opinion of the European Data Protection Supervisor 03/21 of 22 February 2021 on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement. https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-conclusion-eu-and-uk-trade-agreement_en

[134] McCann, Duncan, Oliver Patel, and Javier Ruiz. 2020. "The Cost of Data Inadequacy." New Economics Foundation. November 23, 2020. https://neweconomics.org/2020/11/the-cost-of-data-inadequacy.

[135] Lachenmann, Matthias. 2019. "Data Transfers between the EU and Japan: An Introduction to the EU's Adequacy Decision on Japan." LinkedIn. July 2, 2019. https://www.linkedin.com/pulse/data-transfers-between-eu-japan-introduction-eus-lachenmann/.

experts - openly critic with the 'regulatory imperialism' of the EU - recalling the role of the UK as an innovation hub and, in particular, as the most fertile incubator of Artificial Intelligence firms in Europe, for which the availability of data is essential[136]. Still, Britain's 'inadequacy' has been highlighted on several occasions and for different reasons.

Some of the pieces of legislation introduced subsequently to the 2016 Brexit referendum for some aspects diverged from the EU's understanding of data protection, starting from the DPA 2018 itself. The debated clause of this Bill is an 'immigration exemption'[137]. Restricting mainly the right to access (and the rights deriving from this like to restrict and object to processing or the right to erasure), this limitation would be allowed in cases in which a data controller decided disclosure would "*prejudice effective immigration control*"[138]. The 'immigration exemption' has been challenged before the UK High Court by the Open Rights Group, denouncing the vagueness of its scope of application. According to them, the wording "*immigration control*" would allow too liberal of an application, including every kind of activity related to immigration, including those not connected to the predominant purpose of national or public security. While the High Court rejected the claim, the Court of Appeal on 26 May 2021 found that the government acted unlawfully, and that the 'immigrant exemption' is incompatible with Article 23 GDPR, providing EU exemptions to the GDPR itself. Considering that the Commission in its draft adequacy decision relied on the High Court judgement to respond to the critics[139], it will be interesting to see its feedback and how it will approach this, probably unexpected, change of circumstances.

Another Act called into question has been the Digital Economy Act 2017 ("DEA 2017), and particularly its conception of personal data. If, for the GDPR, data are 'personal' when the data subject can be "singled out"[140], for Article 40(6) DEA 2017 information identifies a specific person if the identity of the person is specified or can be deduced (by itself or with other information) from these. This slight deviation from the GDPR definition can have the effect of expanding the sharing and usage of personal data outside its area of applicability, failing to award an 'essentially equivalent' protection[141]. This argument was quickly

---

[136] Castro, Daniel, and Eline Chivot. n.d. "Not Granting GDPR Adequacy to the UK Would Be a Mistake." Accessed May 28, 2021. https://iapp.org/news/a/not-granting-gdpr-adequacy-to-the-uk-would-be-a-mistake/.

[137] *See* Schedule 2 Part 1 Paragraph 4 of the Data Protection Act 2018.

[138] Rice, Matthew. 2018. "What Is at Stake with the Immigration Exemption Legal Challenge?" Open Rights Group. August 3, 2018. https://www.openrightsgroup.org/blog/what-is-at-stake-with-the-immigration-exemption-legal-challenge/.

[139] Draft Commission Implementing Decision published on 19 February 2021 pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. Recitals 62-65.

[140] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Recital 26.

[141] Korff, Douwe, and Ian Brown. 2020. "The Inadequacy of UK Data Protection Law Part One: General Inadequacy." https://www.ianbrown.tech/wp-content/uploads/2020/10/Korff-and-Brown-UK-adequacy.pdf.

liquidated by the Commission in its Draft[142], as they also did with the complaint on the weak enforcement of data protection rules[143], in the second case stressing the enforcement powers of the Information Commissioner's Office ("ICO), UK's DPA.

One of the most controversial matters of the Draft adequacy decision is the potential onward transfer to third countries lacking adequacy, particularly the United States. The aforementioned 'Five Eyes' agreement, originated to exchange mainly signal intelligence, is of particular concern as it currently provides for an exchange by default of all intelligence material[144]. Among the Five Eyes, as it could be expected, the States with the closest relationship are the UK and the USA: the concern is evident because, even if in the end the UK will be considered as ensuring adequate standards of protection, the US probably won't, at least in the short-medium term. Still, this is not the only way European data may unlawfully reach the US: in the UK GDPR is enshrined the possibility for Her Majesty's Government to issue adequacy decisions themselves once the interim period is over. Because of the commercial (and non-commercial) relations between the two states, and for the commitments the UK made on free flow of data, this could soon be a reality that the EU will need to face[145].

Among others, the EPDB[146] brought attention to the UK-US Cloud Act Agreement[147], a covenant obliging the Parties to remove barriers in their domestic laws so that their national security and law enforcement agencies may obtain certain electronic data directly from the Communications Service Providers ("CSPs) located within the jurisdiction of the other Party[148]. This agreement is an 'executive agreement', a fast-track alternative to Mutual Legal Assistance Treaty ("MLAT), and can be considered as an overseas extension of the US Clarifying Lawful Overseas Use of Data Act ("CLOUD Act) of 2018[149], which essentially

---

[142] Draft Commission Implementing Decision published on 19 February 2021 pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. Recitals 142-143.

[143] *Ibid*. Recitals 92-98.

[144] Korff, Douwe, and Ian Brown. 2020. "The Inadequacy of UK Data Protection Law Part Two: UK Surveillance." https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-Part-Two-DK-IB201130.pdf.

[145] Korff, Brown. 2020. "The Inadequacy of UK Data Protection Law Part One: General Inadequacy."

[146] Letter of the European Data Protection Board to the European Parliament of 15 June 2020 regarding the agreement between the UK and the US on Access to Electronic Data for the Purpose of Countering Serious Crime. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf

[147] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime. Washington, 3 October 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

[148] Anderson, Berengaut, Garland, Hansen, and Peets. 2019. "U.S. and U.K. Sign CLOUD Act Agreement." Inside Privacy. October 11, 2019. https://www.insideprivacy.com/surveillance-law-enforcement-access/10167/.

[149] Text - S.2383 - 115th Congress (2017-2018): CLOUD Act. https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

asserts that US data and communication companies must provide stored customers' data on any server they operate when requested, also providing mechanisms to reject or challenge these if they believe the request violates the privacy rights of the foreign country the data is stored in. EDPB's concerns on onward transfer to the US are reasonable, as the presence of an adequacy decision is likely to allow transfers from the EU to the same UK servers to which the US may resort. In this case, the Commission manages to justify its decision by calling in the EU-US 'Umbrella Agreement'[150], a Treaty of 2016 on data protection in the area of law enforcement cooperation, although not specifically clarifying how this would shield European data from unlawful onward transfers[151].

Going straight to the cause of invalidation of the US adequacy decision, national security and surveillance laws, it may be noted that applying strictly the *Schrems II* reasoning to UK regulations in the same field it's unlikely that they'd withstand it. The national intelligence agency of the UK, the GCHQ, it's notorious for being involved in this mass interception and analysis of data, in addition to being very close to US respective agencies entrusted with the same or similar tasks. It has been advanced that the GCHQ makes massive use of data mining technologies, extracting useful information from big data, for the purposes related to law enforcement as identification of potential terrorists[152]. As it might be expected, the state of the art of these technologies does not allow humans to blindly trust them because of the high level of false positives or negatives, so their application in this area needs to be handled with care[153]. *Schrems II* clearly established that legal basis should provide a clear definition of the scope of limitations to fundamental rights for the sake of an overriding interest: the UK identified such legal basis in the Investigatory Powers Act 2016 ("IPA 2016), allowing bulk extraction of metadata. Other than being in contrast with the principles on indiscriminate retention set out by the CJEU in *La quadrature du Net*[154], it has been argued that it does not set out principles for the restriction of the data mining and AI-based analytical processing activities[155]. Even in this case the Commission, after a thorough assessment of UK's legislation and statements on privacy and data protection[156], found a way to justify its adequacy: IPA 2016

[150] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences. Signed in Amsterdam on 2 June 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN

[151] Kristakis, Theodore, and Kenneth Propp. 2020. "The Legal Nature of the UK-US CLOUD Agreement." Cross-Border Data Forum. April 20, 2020. https://www.crossborderdataforum.org/the-legal-nature-of-the-uk-us-cloud-agreement/.

[152] Korff, and Brown. 2020. "The Inadequacy of UK Data Protection Law Part Two: UK Surveillance."

[153] Schneier, Bruce. 2006. "Why Data Mining Won't Stop Terror." Wired, March 9, 2006. https://www.wired.com/2006/03/why-data-mining-wont-stop-terror-2/.

[154] Judgment of the Court of 6 October 2020, La Quadrature du Net and Others v Premier ministre and Other, C-511/18, ECLI:EU:C:2020:791.

[155] Smith, Graham. 2020. "Hard Questions about Soft Limits." *Cyberleagle* (blog). October 15, 2020. https://www.cyberleagle.com/2020/10/hard-questions-about-soft-limits.html.

[156] Draft Commission Implementing Decision published on 19 February 2021 pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. Recitals 112-265.

is allegedly both establishing sufficient safeguards and providing individuals with administrative and judicial redress.

While IPA is being challenged by civil liberties groups[157], UK's mass interception programmes have been recently declared unlawful by the ECtHR[158]. The judgement of 25 May 2021, a revision of *Big Brothers Watch* before the Grand Chamber[159], found that such programmes have breached the right to privacy and freedom of expression for decades, and for the lack of enforcement powers of the Council of Europe it's very likely that it won't change much in practice; nonetheless, the ongoing procedure for an adequacy decision from the EU can be affected by this judgement and it needs to take it into account.

Although not extensively addressed in this sub-chapter, even in the case of the UK all the tools residual to adequacy decisions for transfers identified under Article 46 GDPR remain as valid options, if implemented with the appropriate post-Schrems modernizations.

Overall, the Schrems judgement set a high threshold of data protection that won't be lowered in the foreseeable future. Some business-friendly commentators have argued that the bar is being set impossibly high[160], and that keeping this standard will hamper EU competitiveness, especially in the innovation sector[161]. If the EU sticks to the mantra "adequacy or nothing", pursuing 'regulatory imperialism' (or, more neutrally, aiming at the cross-fertilisation of data protection regulations), the long term risk is to be isolated and fall behind in the digital economy.

[157] Big Brother Watch team. 2021. "UK Mass Surveillance Found Unlawful by Europe's Highest Human Rights Court — Big Brother Watch". May 25, 2021. https://bigbrotherwatch.org.uk/2021/05/uk-mass-surveillance-found-unlawful-by-europes-highest-human-rights-court/.

[158] Siddique, Haroon. 2021. "GCHQ's Mass Data Interception Violated Right to Privacy, Court Rules." The Guardian. May 25, 2021. http://www.theguardian.com/uk-news/2021/may/25/gchqs-mass-data-sharing-violated-right-to-privacy-court-rules.

[159] Judgement of the European Court of Human Rights of 25 May 2021, Big Brother Watch and Others v. the United Kingdom, application nos. 58170/13, 62322/14 and 24969/15.

[160] Duhs, Eleonor. 2020. "EU-UK Data Flows, Adequacy and Regulatory Changes from 1st January 2021." LinkedIn. December 28, 2020. https://www.linkedin.com/pulse/eu-uk-data-flows-adequacy-regulatory-changes-from-1st-eleonor-duhs/.

[161] Castro, Chivot. 2020. "Not Granting GDPR Adequacy to the UK Would Be a Mistake.".

3. The trend towards data localization

3.1 Data localization and sovereignty

When technologies like the internet and data networks began to emerge, they grew faster than usual technological development. For its nature, the internet connects the world and permits the global exchange of information: the worldwide reach of these new technologies fostered the idea that a new world, an online world with no borders and where power is decentralised, was possible. The potentialities of the World Wide Web have been supported by many at the outset, even declaring that the digital world could cancel or limit many corruptions of the physical and State-based one. The poet and activist for digital rights John Barlow in 1996 even wrote a 'Declaration of Independence of the Internet'[162], a visionary manifesto in which he invites governments not to intrude in online affairs; to them he asserts: "*You are not welcome among us. You have no sovereignty where we gather*". Ironically, that doesn't seem to be the trend 25 years later, when sovereignty over online communications is being fully exercised.

While the notion of sovereignty over *internal* national communications is universally recognised, and should not be questioned, the extraterritorial component of such a notion (manifested through the surveillance programmes seen above) and 'data sovereignty' (subjecting data to the law and governance structures of the nation where they are collected[163]) both contributed to the formation of 'data localization' policies.

Data localization policies enacted so far can be broken in two groups: when a government compel internet content hosts to store data in their jurisdiction they take the name of 'localized data hosting', whereas if the same government compels internet service providers to route data packets (sent and received by users located under the same jurisdiction) only on networks located within their jurisdiction are named 'localized data routing'[164]. Another classification effort that can be done concerning these policies is the one between 'broad' and 'narrow' data localization policies: the distinction between the two lies in the fact that the former usually have general application to all the users and the types of data, while the seconds present some limitations in the application field[165]. In any of these cases, the general underlying idea is to "*move data away from the geographically unbordered world of cyberspace, and plant data directly under local jurisdictions*"[166].

Another line can be drawn between countries enacting data localization strategies based on the previous classification. Only a limited number of

---

[162] Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." Electronic Frontier Foundation. February 8, 1996. https://www.eff.org/cyberspace-independence.

[163] Taylor, Richard D. 2020. "'Data Localization': The Internet in the Balance." *Telecommunications Policy* 44 (8): 102003. https://doi.org/10.1016/j.telpol.2020.102003.

[164] Selby, John. 2017. "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?" *International Journal of Law and Information Technology* 25 (3): 213–32. https://doi.org/10.1093/ijlit/eax010.

[165] *Ibid.*

[166] Taylor, 2020. "'Data Localization': The Internet in the Balance."

countries, including the People's Republic of China and the Russian Federation, enacted broad arrangements, while other countries, among which the EU Member States and the EU itself, are gradually introducing narrow ones[167]. If the adoption of data localization policies *per se* underlines a shared attraction toward data sovereignty, the different degree of application of such rules reflects how the need to protect citizens' data from foreign intrusion is positioned in the scale of priorities. Indeed, the protection of privacy is one of the most common justifications for data localization, but it isn't the only one: national security and economic development have also been recognised as interests protected by it[168]. These being the objectives on paper, it is interesting to analyze how appropriate these measures are to the pursuit of such goals.

As far as national security is concerned, data localization could have beneficial effects. It would be correct to say that governments have spied on each other for centuries, and a confirmation that this practice has not stopped has come from Snowden's revelations. Not only enemies, but allies as well are within the scope of US espionage[169]. Implementing data localization in a country to defend from foreign intrusion may have a favorable and a counterproductive effect. The positive argument is based on the assumption that the performance of mass surveillance strategies is cheaper and more effective when such data can be collected directly from underwater cables or if they are collected while in transit. Data localization would raise the costs of the acquisition of signal intelligence by avoiding flows to third countries, having a dissuasive effect[170]. On the other hand, such policies constrict 'national' data on one or few data centers, that would become 'honeypots'[171]; this applies not only to foreign intelligence agencies, but also to malevolent hackers and criminals. Data localization, in addition, limits to a certain extent obfuscation practices, among which 'data sharding'. This common practice implies that no single data center stores all the data required to reassemble a document, which are instead fragmented and kept in a multitude of them, so that in case of adverse occurrences the information itself is not compromised[172]. The same argument is valid also for the goal of protection of privacy of citizens from foreign mass surveillance.

With regard to economic development, instead, data localization presents many flaws: in simple terms, it harms economic efficiency in several ways. Being these policies *de facto* protectionist ones, they imply both a stimulus to some businesses (in this case the relatively small cloud storage business) and an

---

[167] Chander, Anupam, and Uyen P. Le. 2015. "Data Nationalism." SSRN Scholarly Paper ID 2577947. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2577947.

[168] *Ibid*.

[169] Levs, Josh, and Catherine E. Soichet. 2013. "Europe Furious, 'shocked' by Report of U.S. Spying." CNN. July 1, 2013. https://www.cnn.com/2013/06/30/world/europe/eu-nsa/index.html.

[170] Selby, 2017. "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?"

[171] Chander, Anupam, and Uyen P. Le. 2014. "Breaking the Web: Data Localization vs. The Global Internet." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2407858.

[172] Ryan, Patrick S., Sarah Falvey, and Ronak Merchant. 2013. "When the Cloud Goes Local: The Global Problem with Data Localization." *Computer* 46 (12): 54–59. https://doi.org/10.1109/MC.2013.402.

increase of costs for many other industries[173]. Most notably, the cloud business does not employ a significant number of persons, and CPUs, motherboards, RAM chips and all the network equipment required to run such an enterprise are produced by few oligopolized undertakings mainly located in China, Taiwan and the US[174]. Furthermore, restrictions of this kind will hamper the possibility of taking advantage of economies of scale: data centers require constant access to power and cooling sources and need to be distant from places where natural disasters - earthquakes, cyclones, etc... - are recurrent[175], that is why some locations on Earth fit these requirements best. It has been also argued that data localization will benefit existing larger companies in a disproportionate way compared to SMEs[176], with an argument similar to the one dealt with when analysing post-Schrems II SCCs; compliance with the regulatory burden introduced by data localization policies would be much more difficult for smaller companies, startups and no-profits and, consequently, the affirmation of these in the global market could become almost impossible.

Rather than bringing economic development to the country that enacts them, data localization policies would engender not indifferent restrictions to trade. Both the DPD[177] and the GDPR were enacted with the aim of fostering trade while ensuring protection of fundamental rights; the latter, in its Recital 101, recognises that: "*Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation*"[178]. It is interesting to note that international trade and cooperation are mentioned together. Possibly, this clause reflect the view set out by Friedman in its 'Golden Arches theory of conflict prevention'[179], according to which countries that trade with each other are less inclined to enter into conflicts and wars. This well-established conception is today complemented by theories on 'weaponized interdependence', according to which economic connections shape networks where power relations can be leveraged to pursue the same goals that once apparteined principally to armed conflicts[180]. In this context in which international power relations highly depend on the trade and

[173] Ferracane, Martina Francesca, Janez Kren, and Erik Marel. 2020. "Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?" *Review of International Economics* 28 (3): 676–722. https://doi.org/10.1111/roie.12467.

[174] "List of Semiconductor Fabrication Plants." 2021. In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=List_of_semiconductor_fabrication_plants&oldid=1026170408.

[175] Bias, Randy. 2010. "Understanding Cloud Datacenter Economies of Scale." Cloudscaling. May 4, 2010. http://cloudscaling.com/blog/cloud-computing/understanding-cloud-datacenter-economies-of-scale/.

[176] Bowman, Courtney. 2017. "Data Localization Laws: An Emerging Global Trend." January 6, 2017. https://www.jurist.org/commentary/2017/01/courtney-bowman-data-localization/.

[177] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Recital 56.

[178] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Recital 101.

[179] Friedman, L. Thomas. 2000. "The Lexus and the Olive Tree". *Anchor books*. 2nd Edition.

[180] Farrell, Henry, and Abraham L. Newman. 2019. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44 (1): 42–79. https://doi.org/10.1162/isec_a_00351.

economic relations among States, restrictions to trade like data localization may be a way of exercising such power. Nonetheless, for the protective nature of these measures and the above analysed costs, it would not be the sharpest move for those who want to leverage their position, and may result in an own goal. Besides, the enactment of such protectionist policies is in itself an invitation to retaliate[181], with the potential risk of an escalation threatening peace. This would confirm Friedman's idea: once economic relations are hindered by data localization, hostilities are likely to increase.

3.2 Cloud services and their post-Schrems II challenges: reconciling data sovereignty and data flows.

The judgement of July 2020 has not been a simple restatement of the first case brought by Schrems. It established that either a transfer is GDPR compliant and ensures the level of protection required by it, or it is not; in that case, the transfer needs to be stopped. The CJEU, well aware of the high data protection standards required by the EU, opened a debate on the future of cross-border transfers that is left to policy makers. Taking into consideration the requirement of stopping non-compliant transfers, the choice the regulator has is twofold.

One option allows and supports data transfers, and aims at developing an international framework in which, either by international law instruments or by national laws, common standards of protection of personal data are set. This is probably the future scenario most desired by the EU institutions. The Commission decided to stick to adequacy decisions as the primary tool to ensure protection in the 2016 reform of data protection regulations, notwithstanding the critics this tool had received[182]. The GDPR proposed itself as a comprehensive Regulation meant to be an inspiration for foreign countries, triggering the 'Brussels effect'[183], the process of *de facto* regulatory globalisation triggered by the EU. The Court, on its side, has shown its proclivity for the raising of global standards of protection as well: they have spent an important part of their reasoning reinforcing and supporting alternatives to adequacy decisions.

The alternative would be data localization: it would be a way of totally avoiding transfers while pursuing the goals of privacy and economic development, as argued by Maximillian Schrems himself[184]; yet, it would be naive not to consider the counter arguments presented above. By deciding that transfers should be stopped when noncompliant, the Court advanced this second hypothesis as well; notwithstanding the open market vocation of the EU, considering the improbability of third States ensuring a level of protection

[181] Chander, 2020. "Is Data Localization a Solution for Schrems II?"

[182] Kuner, Christopher. 2009. "Developing an Adequate Legal Framework for International Data Transfers." In *Reinventing Data Protection?*, edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt, 263–73. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-1-4020-9498-9_16.

[183] Bradford, Anu. 2020. "The Brussels Effect." In *The Brussels Effect*, by Anu Bradford, 25–66. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.003.0003.

[184] Fennessy, Caitlin, Maximillian Schrems, and Eduardo Ustaran. 2020. *The Schrems II Decision: The Day After*. https://www.linkedin.com/video/live/urn:li:ugcPost:6689891492103798784/

'essentially equivalent' to the one of the EU because of its significance, and adding up the fact that *Schrems II* burdened undertakings with more obligations, the option of keeping EU data in the EU jurisdiction should not be relinquished.

It is in this framework that cloud computing is growing fast, and is expected to become the mainstream form of computing in the future. Until a few years ago, the world had relied on decentralized computing, meaning that data was stored and software was run on the device itself. In few words, cloud computing shifts data and applications on shared data centers with enormous capacities of storage and processing power, exploiting the benefits of economies of scale, lowering costs, and allowing new applications of computing[185]. Being it a a virtual, dynamic technology[186] operating globally, the question on transborder data access is soon raised[187]: regulating the access to web farms situated in different countries is gradually becoming a necessity.

One of the first legal complications with cross-border transfers from a cloud server located on a third country arose already in 2013, in the renowned *Microsoft* case[188]. The company challenged an FBI warrant, issued by a judge of the Southern District of New York, requiring the handing over of emails of a presumed international drug trafficker, partially stored in Ireland. Microsoft's argument was that US internal law (in this case, the Stored Communication Act, "SCA) wasn't applicable to data located in a territory different from theirs; to prove their point, they promptly delivered the portion of information requested that were stored in the US jurisdiction. After losing in the first instance Court, as it concluded that for the nature of the applicable provision it could not be constrained by territorial restrictions, Microsoft appealed to the Second Circuit Court. The latter in 2016 ruled in favor of Microsoft, invalidating the warrant and sustaining that for the purposes of the SCA such information should have been obtained by triggering the MLAT already in force between the USA and Ireland[189]. In return, the US Department of Justice appealed to the Supreme Court of the United States the next year, but a ruling was never issued because in the meanwhile the US Congress passed the well-known CLOUD Act, amending the SCA[190]. Because of this, the judgement of the appeal court was vacated - that is, rendered invalid - and sent back to the Second District Court where it was declared moot, meaning that a live dispute lacked between the parties and there was no need to go further in proceedings. The newly introduced provision, indeed, permitted governments to govern exchanges of informations through executive agreements and allows

---

[185] Irion, Kristina. 2012. "Government Cloud Computing and National Data Sovereignty: Government Cloud Computing and National Data Sovereignty." *Policy & Internet* 4 (3–4): 40–71. https://doi.org/10.1002/poi3.10.

[186] Mell, Peter, and Tim Grance. 2019. "The NIST Definition of Cloud Computing." National Institute of Standards and Technology. www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

[187] Alì, Antonino. 2016. "Lo Stato, il Territorio, l'Accesso e la Localizzazione dei Dati ai Tempi del Cloud Computing," 4.

[188] United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018).

[189] Ellingsen, Nora. 2016. "The Microsoft Ireland Case: A Brief Summary." Lawfare. July 15, 2016. https://www.lawfareblog.com/microsoft-ireland-case-brief-summary.

[190] Brandom, Russell. 2018. "House Passes Controversial Legislation Giving the US More Access to Overseas Data." The Verge. March 22, 2018. https://www.theverge.com/2018/3/22/17131004/cloud-act-congress-omnibus-passed-mlat.

the warrants to be challenged considering the location, nationality and connection to the US of the data subject[191].

The *Microsoft* case raised some interesting points concerning cloud storage and access to data stored in a foreign country. Still, being the context the one of law enforcement, the prominence of the aim pursued and the presence of instruments like MLATs ease the perception of intrusiveness that a different way of accessing data, namely foreign surveillance, could give. Being cloud companies' data centers located within the jurisdiction of a State, it would be reasonable to think that States that are not new to mass surveillance would try to exploit data centers on their territory, as they already did in the past, to collect data for those purposes. Nonetheless, the dimension of foreign surveillance can be said to have a global scope, as shown by strategic bulk collection (UPSTREAM programme), international agreement for the systematic sharing of the collected data (Five Eyes) and occasional bilateral cooperations. The latter is recently being discussed: the new revelations on the role played by Denmark in 2013 tapping of European leaders shocked both EU and Member States' institutions[192]. Some have argued that, because of the subtle and worldwide dimension of surveillance, the geographical feature loses relevance in favour of a different kind of protection: technical data protection[193]. As it was the case for post-*Schrems II* transfers, also for data at rest the solution may come from a strong level of encryption or other technical measures.

With data protection and security awareness growing more and more among the public, both the location of data centers and the degree of technical protection are becoming competitive parameters of choice among consumers[194]. That is why in the latest years telecommunication companies have concluded agreements and arranged their networks to reflect both the privacy and security concerns of the consumers and the data localization requirements coming from national institutions.

Germany is not among the countries having enacted broad data localization policies, but nonetheless Deutsche Telekom - a State-owned telecommunication company[195] - restructured its network to ensure that the main hubs and are strategically located on German territory in order for German data not to transit in third countries[196]. In 2015 the same company concluded an agreement with Microsoft to provide German Azure and Office 365 users with the possibility of

[191] Chander, 2020. "Is Data Localization a Solution for Schrems II?"
[192] Vinocur, Nicholas, Rym Momtaz, and Mark Scott. 2021. "Snowden's Back: Spying Scandal Clouds EU-US Ties Ahead of Biden Visit." POLITICO. May 31, 2021. https://www.politico.eu/article/edward-snowden-is-back-spying-scandal-disrupts-eu-us-ties-ahead-of-joe-biden-europe-visit/.
[193] Millard, Christopher. 2015. "Forced Localization of Cloud Services: Is Privacy the Real Driver?" *IEEE Cloud Computing* 2 (2): 10–14. https://doi.org/10.1109/MCC.2015.37.
[194] *Ibid*.
[195] "Deutsche Telekom." 2020. In *Wikipedia*. https://it.wikipedia.org/w/index.php?title=Deutsche_Telekom&oldid=115129630.
[196] Alì, 2016. "Lo Stato, il Territorio, l'Accesso e la Localizzazione dei Dati ai Tempi del Cloud Computing,"

having their data kept in their own country on Deutsche Telekom facilities[197]. The latter had been bestowed with the role of 'data trustee', responsible for controlling and overseeing all access to customer data; the novelty of this system was that Microsoft was allowed access to these data only in contractually compliant cases[198]. This service was discontinued in 2018 on the grounds that "*customers' needs have shifted, and the isolation of Microsoft Cloud Germany imposes limits on its ability to address the flexibility and consistency customers desire today*"[199]; the functional substitute to the data trustee system has been a cloud service reliant on new Microsoft-owned data centers located in Germany[200]. From the standpoint of data sovereignty, the two situations are very different. Although data residency (the storage of data in the country one wishes) can still be ensured to end users, the new service offered is short of the guarantees on access that a data trustee arrangement was capable of safeguarding. The data trustee experiment remains a viable way to balance the exercise of data sovereignty of States with the need for data to flow reasonably without hindrances, being the only argument against the unclarified change in needs of end users advanced by Microsoft.

In any case, this is not the only attempt to find a manageable solution to balance the two goals: another feasible option could be the 'federated' model[201]. This is based on the assumption that rules on data transfers should follow a risk-based approach, meaning that depending on their sensitivity data should be more or less paid attention in transfers[202]. The federated model applies to data pertaining to the highest level of sensitivity, and suggests keeping these data sets within the boundaries of the sovereign State while granting access on request to the accredited applicants. This scheme is 'federated' because notwithstanding the different locations where the chosen data sets are stored, these are virtually connected and can be accessed through the same software interface[203]. This system is put in practice by the Global Alliance for Genomics and Health since 2013[204].

A third system that tries to conciliate privacy and business needs is the one of 'data embassies'. Although it takes many shapes and could be implemented for different reasons, generally speaking the notion of 'embassy' implies having a

---

[197] Microsoft Reporter. 2015. "Microsoft Announces Plans to Offer Cloud Services from German Datacenters." Microsoft News Centre Europe. November 11, 2015. https://news.microsoft.com/europe/2015/11/11/45283/.

[198] Wigand, Ralf, and Julia Kornich. 2020. "Azure Germany Data Trustee." October 16, 2020. https://docs.microsoft.com/en-us/azure/germany/germany-overview-data-trustee.

[199] Dedezade, Esat. 2018. "Microsoft to Deliver Cloud Services from New Datacentres in Germany in 2019 to Meet Evolving Customer Needs." Microsoft News Centre Europe. August 31, 2018. https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/.

[200] Keane, Tom. 2019. "Microsoft Azure available from new cloud regions in Germany." September 9, 2019. https://azure.microsoft.com/it-it/blog/microsoft-azure-available-from-new-cloud-regions-in-germany/.

[201] Fan, Ziyang, and Anil K. Gupta. 2018. "The Dangers of Digital Protectionism." *Harvard Business Review*, August 30, 2018. https://hbr.org/2018/08/the-dangers-of-digital-protectionism.

[202] *Ibid*.

[203] Goodhand, Peter. 2016. "A Federated Ecosystem for Sharing Genomic, Clinical Data." *Science* 352 (6291): 1278–80. https://doi.org/10.1126/science.aaf6162.

[204] *Ibid*.

foreign data center where data coming from a different State are stored safely. Data embassies have been proposed or implemented with two facets: a public/institutional one and a private one, developed after *Schrems II*.

The first and original has its genesis in Estonia, a country known to be a leader in digital innovation. Estonia managed to develop a whole Government Cloud System, setting up two governmental data centers within their territory and several data embassies across the world[205]. While the most sensitive data are and will be stored on Estonian soil, to avoid foreign surveillance, there are important data sets which need to be backed up or stored on a different territory without that degree of sensitivity, and that's where the data embassies system steps in. Such system arises both from the digital vocation of the country and the 2014 aggressive turn of Russia towards Ukraine[206]: digital continuity became an essential feature for the country, either for commerce or security purposes. The team working on the project envisioned both 'virtual' and 'physical' Data Embassies[207]: the former consist in the storage of data, adequately protected in advance with technical measures, on foreign countries' territory and within private companies facilities; the latter, instead, entails the storage of such data within the Estonian embassies (or the ones of friendly countries). This last option has been criticised: the concentrations of few sensitive informations in a known place could easily make it become target of a cyberattack (in addition, data are less secure there than in a privately owned web farm)[208].

The second is a byproduct of the Schrems II judgement, and comes particular from a specific company, Anonos[209]. In a Memorandum[210] submitted to the EDPB, the application of the 'Data Embassy Principles' was proposed as a supplementary measure, to be read with *Schrems II* meaning. In concrete terms, they borrowed the idea of the Estonian Virtual Data Embassy, applied it to privates by subjecting transfers to the Data Embassy Principles, which are meant to render the data transfer GDPR and *Schrems II* compliant. The said principles are: GDPR Pseudonymisation, Data Minimisation, Secured Personal Data (by making it impossible to link the information transferred to the data subject to which those data pertain), Demonstrability and Responsibility[211]. In practice, allegedly, this system of protection should allow the protection of data while in use: by keeping the additional information to link the information to the data subject located on EU servers, pseudonymisation could be GDPR effective as an outcome of the transfer.

It is soon to establish if any of these models could become predominant in the near future, if any of these will. What is foreseeable is that technical data

---

[205] Kotka, Taavi, and Innar Liiv. 2015. "*Concept of Estonian Government Cloud and Data Embassies"*. Vol. 9265. Lecture Notes in Computer Science. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-22389-6.

[206] Kaljund, A. Lorraine. 2018. "Restoration Doctrine Rebooted: Codifying Continuity in the Estonian Data Embassy Initiative." *PoLAR: Political and Legal Anthropology Review* 41 (1): 5–20. https://doi.org/10.1111/plar.12240.

[207] *Ibid*.

[208] Kotka, Innar. 2015. "*Concept of Estonian Government Cloud and Data Embassies"*

[209] Anonos. n.d. "Anonos | How Anonos Started." Accessed June 14, 2021. https://www.anonos.com/how-anonos-started.

[210] Feys, Magali and LaFever, Gary. 2020. Memorandum. https://www.dataembassy.com/

[211] *Ibid.*

protection standards will improve, also as a consequence of *Schrems II* and its additional safeguards clause. The use of techniques like pseudonymisation, nonetheless, is threatened by a disruptive innovation: quantum computing. With its enormous computing power, it is expected to shake all the grounds on which we are standing now as far as concerns techniques of data securitization.

Conclusions

The *Schrems II* judgement poses a medium-long term challenge for the Commission, which can be dealt with through a variety of means to be chosen by the policy makers. The CJEU, though, did not leave undertakings in the darkness. While invalidating the most comprehensive instrument for cross-border transfers to the US, the Privacy Shield adequacy decision, it establishes clear parameters for transfers through other means in a way that is burdensome, but also flexible. The 'additional safeguards' required by the judgement (where opportune) can take a variety of shapes to protect data in the most appropriate way and adapt to innovations in the digital field, as seen with cloud computing, respecting the EU level of protection.

The Commission, aware of the high GDPR standards, is continuing to push towards the adoption of an adequacy decision for the United Kingdom, notwithstanding the many criticisms advanced and the likelihood that the Court will strike it down as they did with the Privacy Shield. The Commission is proceeding with blinders on, manifesting the political will not to miss the opportunities of the innovation market which calls for a liberal approach to data flows. The Court, on the other hand, guards the uniformity of the protection of personal data, and it's implausible that it will disacknowledge its bold decision in *Schrems II*.

Leaving aside the EU and its particular apprehension for the rule of law, the rest of the world is moving forward, with some States enacting broad data localization policies. Taking also this trend in consideration, the long-term future scenarios that can be prefigured are three-pronged. The first, and less plausible, is that the EU will enact data localization policies as well, joining the global trend and keeping the degree of protection of EU citizens' data significant as it is today. Secondly, the Commission could lower the standards of protection awarded to data transferred to third countries, lessening the extraterritorial overreach of the GDPR and alining itself to other less restrictive countries, like the UK; this trade-friendly measure would allow it to issue adequacy decision that could stand the CJEU test. The third scenario, the most desirable and plausible at the moment, is a situation in which the EU succeeds in applying its level of protection to outwards cross-border transfers, either as a consequence of the introduction of new regulations in the receiving country or because of the consolidation of the 'additional safeguard' method; the protection of data through effective technical measures could be the best method of protecting data while ensuring their free flow, independently of the regulatory framework of the third State.

Bibliography

Scientific literature

Alì, Antonino. n.d. “Lo Stato, il Territorio, l’Accesso e la Localizzazione dei Dati ai Tempi del Cloud Computing”.

Anderson, Berengaut, Garland, Hansen, and Peets. 2019. “U.S. and U.K. Sign CLOUD Act Agreement.” Inside Privacy. October 11, 2019.

Barlow, John Perry. 1996. “A Declaration of the Independence of Cyberspace.” Electronic Frontier Foundation. February 8, 1996.

Bias, Randy. 2010. “Understanding Cloud Datacenter Economies of Scale.” Cloudscaling. May 4, 2010.

Big Brother Watch team. 2021. “UK Mass Surveillance Found Unlawful by Europe’s Highest Human Rights Court.” Big Brother Watch. May 25, 2021.

Bignami, Francesca. 2020. “Schrems II: The Right to Privacy and the New Illiberalism.” Verfassungsblog (blog). July 29, 2020.

Bowman, Courtney. 2017. “Data Localization Laws: An Emerging Global Trend.” January 6, 2017.

“Bradford, Anu. 2020. “The Brussels Effect.” In *The Brussels Effect*, by Anu Bradford. Oxford University Press.

Brandom, Russell. 2018. “House Passes Controversial Legislation Giving the US More Access to Overseas Data.” The Verge. March 22, 2018.

Brkan, Maja. 2018. “The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core.” *European Constitutional Law Review.*

———. 2019. “The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU’s Constitutional Reasoning.” *German Law Journal* 20 (6): 864–83.

Bulao, Jacquelyn. 2020. “How Much Data Is Created Every Day in 2021?” TechJury. June 24, 2020.

Castro, Daniel, and Eline Chivot. 2020. “Not Granting GDPR Adequacy to the UK Would Be a Mistake.” September 14, 2020.

Chander, Anupam. 2020. “Is Data Localization a Solution for Schrems II?” SSRN Scholarly Paper ID 3662626. Rochester, NY: Social Science Research Network.

Chander, Anupam, and Uyen P. Le. 2014. “Breaking the Web: Data Localization vs. The Global Internet.” *SSRN Electronic Journal*.

———. 2015. “Data Nationalism.” SSRN Scholarly Paper ID 2577947. Rochester, NY: Social Science Research Network.

Church, Peter, and Georgina Kon. 2021. “Brexit: Where Does the Adequacy ‘Bridge’ Lead To?” Linklaters.

Clark, Sam. 2020. “Schrems II Hub: Every Development in the Saga.” Global Data Review. November 2, 2020.

Cory, Nigel, Daniel Castro, and Ellysse Dick. 2020. “‘Schrems II’: What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation.” Information Technology and Innovation Foundation.

Daskal, Jennifer, and Peter Swire. 2019. “The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards.” Lawfare. October 8, 2019.

Dedezade, Esat. 2018. “Microsoft to Deliver Cloud Services from New Datacentres in Germany in 2019 to Meet Evolving Customer Needs.” Microsoft News Centre Europe. August 31, 2018.

Dhont, Jan Xavier. 2019. “Schrems II. The EU Adequacy Regime in Existential Crisis?” *Maastricht Journal of European and Comparative Law.*

Digital Europe. 2020. “An Early Analysis of Schrems II – Key Questions and Possible Ways Forward.”

Duhs, Eleonor. 2020. “EU-UK Data Flows, Adequacy and Regulatory Changes from 1st January 2021.” LinkedIn. December 28, 2020.

Edgington, Tom. 2020. “Brexit: What Are the Key Points of the Deal?” *BBC News*, December 30, 2020.

Ellingsen, Nora. 2016. “The Microsoft Ireland Case: A Brief Summary.” Lawfare. July 15, 2016.

Étienne Armingaud, Claude. 2020. “EU Data Protection: In a Post-Privacy Shield, Sectorial Code of Conduct Could Lead the Way to Safeguard Data Transfers Outside the EU/EEA.” K&L Gates. July 17, 2020.

EU Cloud Coc. n.d. “Complementing the EU Cloud CoC to Become a Safeguard Pursuant Art. 46 GDPR.”.

Fabbrini, Federico. n.d. “Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States.” Koninklijke Brill NV.

Fallows, James. 2008. “The Connection Has Been Reset” The Atlantic. March 2008.

Fan, Ziyang, and Anil K. Gupta. 2018. “The Dangers of Digital Protectionism.” Harvard Business Review, August 30, 2018.

Farrell, Henry, and Abraham L. Newman. 2019. “Weaponized Interdependence: How Global Economic Networks Shape State Coercion.” *International Security.*

Fennessy, Caitlin, Maximillian Schrems, and Eduardo Ustaran. 2020. “*The Schrems II Decision: The Day After*”. July 2020.

Ferracane, Martina Francesca, Janez Kren, and Erik Marel. 2020. “Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?” *Review of International Economics.*

Friedman, L. Thomas. 2000. “The Lexus and the Olive Tree”. Anchor books. 2nd Edition.

Goodhand, Peter. 2016. “A Federated Ecosystem for Sharing Genomic, Clinical Data.” *The Global Alliance for Genomics and Health.*

Greenwald, Glenn. 2014. *Sotto Controllo. Edward Snowden e La Sorveglianza Di Massa*. Rizzoli.

Irion, Kristina. 2012. “Government Cloud Computing and National Data Sovereignty: Government Cloud Computing and National Data Sovereignty.” *Policy & Internet.*

Jones, Edward. 2021. “AWS vs Azure in 2021 (Comparing the Cloud Computing Giants).” Kinsta. March 25, 2021.

Kaljund, A. Lorraine. 2018. “Restoration Doctrine Rebooted: Codifying Continuity in the Estonian Data Embassy Initiative.” *PoLAR: Political and Legal Anthropology Review.*

Kamara, Irene. 2020. “4 GDPR-Certification Myths Dispelled.” January 28, 2020.

Kask, Laura, and Nick Robinson. n.d. “The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis.”

Keane, Tom. 2019. “Microsoft Azure available from new cloud regions in Germany.” September 9, 2019.

Klovig Skelton, Sebastian. 2020. “Over Half of Firms Intend to Continue US Data Transfers despite Schrems II.” ComputerWeekly.Com. September 23, 2020.

Kong, L. 2010. “Data Protection and Transborder Data Flow in the European and Global Context.” *European Journal of International Law*.

Korff, Douwe, and Ian Brown. 2020a. “The Inadequacy of UK Data Protection Law Part One: General Inadequacy.” October 9, 2020.

———. 2020b. “The Inadequacy of UK Data Protection Law Part Two: UK Surveillance.” November 30, 2020.

Kotka, Taavi, and Innar Liiv. 2015. *Concept of Estonian Government Cloud and Data Embassies*. Springer International Publishing.

Kristakis, Theodore. 2020. “After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe.” *European Law Blog* (blog). July 21, 2020.

Kristakis, Theodore, and Kenneth Propp. 2020. “The Legal Nature of the UK-US CLOUD Agreement.” Cross-Border Data Forum. April 20, 2020.

Kuner, Christopher. 2009a. “Developing an Adequate Legal Framework for International Data Transfers.” In *Reinventing Data Protection?*, edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt. Springer Netherlands.

———. 2020. “The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation.” *European Law Blog* (blog). July 17, 2020.

Lachenmann, Matthias. 2019. “Data Transfers between the EU and Japan: An Introduction to the EU’s Adequacy Decision on Japan.” LinkedIn. July 2, 2019.

Lenaerts, Koen. 2019. “Limits on Limitations: The Essence of Fundamental Rights in the EU.” *German Law Journal.*

Levs, Josh, and Catherine E. Soichet. 2013. “Europe Furious, ‘shocked’ by Report of U.S. Spying.” CNN. July 1, 2013.

Lubin, Asaf. 2017. “A New Era of Mass Surveillance Is Emerging Across Europe”. January 9, 2017.

Lynskey, Orla. 2014. “Deconstructing data protection: the ‘added-value’ of a right to data protection in the EU legal order.” *International and Comparative Law Quarterly.*

Maisse, Odile, Giulio Sabbati, and Laura Bartolini. 2016. “US: Economic Indicators and Trade with the EU”.

Manancourt, Vincent. n.d. “EU’s Rejection of US Surveillance Also Tests Its Commitment to Privacy.” Politico.

Massé, Estelle. 2021. “Access Now’s Memo on the Data Transfers and PNR Provisions under the EU-UK Trade Agreement.” AccessNow.

McCann, Duncan, Oliver Patel, and Javier Ruiz. 2020. “The Cost of Data Inadequacy.” New Economics Foundation. November 23, 2020.

Mell, Peter, and Tim Grance. 2019. “The NIST Definition of Cloud Computing.” National Institute of Standards and Technology.

Meltzer, Joshua. 2015. “Hearing on ‘Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows.’”

Microsoft Reporter. 2015. “Microsoft Announces Plans to Offer Cloud Services from German Datacenters.” Microsoft News Centre Europe. November 11, 2015.

Mildebrath, Hendrik. 2020. “The CJEU Judgment in the Schrems II Case.” European Parliamentary Research Service. September 2020.

———. 2021. “EU-UK Private-Sector Data Flows after Brexit: Settling on Adequacy.” European Parliamentary Research Service. April 2021.

Millard, Christopher. 2015a. “Forced Localization of Cloud Services: Is Privacy the Real Driver?” *IEEE Cloud Computing.*

Mishra, Neha. 2020. “Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?” *World Trade Review.*

Mitsilegas, Valsamis. 2020. “The Preventive Turn in European Security Policy: Towards a Rule of Law Crisis?” In *EU Law in Populist Times*, edited by Francesca Bignami. Cambridge University Press.

Monteleone, Shara, and Laura Puccio. 2015. “The CJEU’s Schrems Ruling on the Safe Harbour Decision.” European Parliamentary Research Service. October 2015.

———. 2016. “The Privacy Shield: Update on the State of Play of the EU US Data Transfer Rules : In Depth Analysis.” European Parliamentary Research Service. July 2018.

———. 2017. “From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU US Data Transfer Rules.” European Parliamentary Research Service. January 2017.

Moody, Glyn. 2021. “Irony Alert: US Could Block Personal Data Transfers To Ireland, European Home Of Digital Giants, Because GDPR Is Not Being Enfor.” *The New York Press News Agency* (blog). April 23, 2021.

Nakashima, Ellen. 2018. “Justice Department Asks Supreme Court to Moot Microsoft Email Case, Citing New Law.” *Washington Post*. March 31, 2018.

Nielsen, Nikolai. 2020. “US Firms Ignoring EU Court Ruling on Data, Schrems Warns.” EUobserver. September 4, 2020.

NOYB. 2020a. “CJEU Invalidates ‘Privacy Shield’ in US Surveillance Case. SCCs Cannot Be Used by Facebook and Similar Companies.” Noyb.Eu. July 16, 2020.

———. 2020b. “Next Steps for EU Companies & FAQs.” Noyb.Eu. July 20, 2020.

———. 2020c. “101 Complaints on EU-US Transfers Filed.” Noyb.Eu. August 17, 2020.

———. 2020d. “Update on Noyb’s 101 Complaints on EU-US Data Transfers.” Noyb.Eu. September 22, 2020.

———. 2020e. “Opening Pandora’s Box: Companies Can’t Say How They Comply with CJEU Ruling.” Noyb.Eu. September 25, 2020.

O’Donoghue, Cyinthia, and Nona Keyhani. 2018. “ECtHR Rules on UK Mass Surveillance under RIPA.” Technology Law Dispatch. October 25, 2018.

Oldani, Isabella. 2020. “The future of data transfer rules in the aftermath of Schrems II.” *SIDIBlog* (blog). October 23, 2020.

Open Rights Group. 2021. “Immigration Exemption Judged Unlawful, Excessive, Wrong by Court of Appeal.” Open Rights Group. May 26, 2021.

Patel, Oliver, and Nathan Lea. 2019. “EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?” UCL European Institute.

Pfisterer, Valentin M. 2019. “The Right to Privacy—A Fundamental Right in Search of Its Identity: Uncovering the CJEU’s Flawed Concept of the Right to Privacy.” *German Law Journal*.

Propp, Kenneth. 2020. “Putting Privacy Limits on National Security Mass Surveillance: The European Court of Justice Intervenes.” *Atlantic Council* (blog). February 21, 2020.

Reidenberg, Joel. 2015. “The data surveillance State in the United States and Europe.” *WAKE FOREST LAW REVIEW*. May 22, 2015.

Reyes, Carla L. 2011. “WTO-compliant protection of fundamental rights: lessons from the EU privacy directive”.

Rice, Matthew. 2018. “What Is at Stake with the Immigration Exemption Legal Challenge?” Open Rights Group. August 3, 2018.

Rotenberg, Marc. 2020. “Schrems II: From Snowden to China: Toward a New Alignment on Transatlantic Data Protection.” *European Law Journal.*

Rotenberg, Marc, and Eleni Kyriakides. 2020. “Preserving Article 8 in Times of Crisis: Constraining Derogations from the European Convention on Human Rights.” In *EU Law in Populist Times*, edited by Francesca Bignami. Cambridge University Press.

Rouvroy, Antoinette, and Yves Poullet. 2009. “The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy.” In *Reinventing Data Protection?*, edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt. Springer Netherlands.

Ruiz, Javier. 2020. “Briefing: How the UK-Japan Trade Deal Severs Post-Brexit Data Adequacy.” Open Rights Group. November 5, 2020.

Ryan, Johnny. 2021. “New Economic Risk: Draft US Senate Bill and Ireland’s GDPR Enforcement.” Irish Council for Civil Liberties.

Ryan, Patrick S., Sarah Falvey, and Ronak Merchant. 2013. “When the Cloud Goes Local: The Global Problem with Data Localization.” *Computer*. April 15, 2021.

Sabbati, Giulio. 2019. “US: Economic Indicators and Trade with EU.”. October 2019.

Sajfert, Juraj. 2020. “Bulk Data Interception/Retention Judgments of the CJEU – A Victory and a Defeat for Privacy.” European Law Blog (blog). October 26, 2020.

Scally, Derek. 2021a. “Irish Approach to Data Protection ‘Kafkaesque’, Says Schrems.” The Irish Times. April 9, 2021.

———. 2021. “US Senate to Debate Limiting Foreign States’ Access to Citizens’ Data.” *The Irish Times*, April 15, 2021.

Schneier, Bruce. 2006. “Why Data Mining Won’t Stop Terror.” *Wired*, March 9, 2006.

Scott, Mark. 2021. “Biden Seeks High-Level Data Deal to Repair EU-US Digital Ties.” Politico. June 2, 2021.

Selby, John. 2017. “Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?” *International Journal of Law and Information Technology*.

Shubber, Kadhim. 2013. “A Simple Guide to GCHQ’s Internet Surveillance Programme Tempora.” *Wired UK*, June 24, 2013.

Siddique, Haroon. 2021. “GCHQ’s Mass Data Interception Violated Right to Privacy, Court Rules.” The Guardian. May 25, 2021.

Smith, Graham. 2020. “Hard Questions about Soft Limits.” *Cyberleagle* (blog). October 15, 2020.

Solove, Daniel. 2015. “Sunken Safe Harbor: 5 Implications of Schrems and US-EU Data Transfer.” TeachPrivacy. October 13, 2015.

Stahl, Titus. 2016. “Indiscriminate Mass Surveillance and the Public Sphere.” *Ethics and Information Technology*.

Taylor, Richard D. 2020. “‘Data Localization’: The Internet in the Balance.” *Telecommunications Policy*.

Tene, Omer. 2020. “The Show Must Go On.” July 17, 2020.

Tracol, Xavier. 2020. “‘Schrems II’: The Return of the Privacy Shield.” *Computer Law & Security Review.*

Turner, Scott. 2008. “Transnational Corporations and The Question of Sovereignty: An Alternative Theoretical Framework for the Information Age.” *Southeastern Political Review*.

Vinocur, Nicholas, Rym Momtaz, and Mark Scott. 2021. “Snowden’s Back: Spying Scandal Clouds EU-US Ties Ahead of Biden Visit.” POLITICO. May 31, 2021.

Wigand, Ralf, and Julia Kornich. 2020. “Azure Germany Data Trustee.” October 16, 2020.

Zeng, Jinghan, Tim Stevens, and Yaru Chen. 2017. “China’s Solution to Global Cyber Governance: Unpacking the Domestic Discourse of ‘Internet Sovereignty’: China’s solution to cyber governance.” *Politics & Policy*.

European Union law

Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences. Signed in Amsterdam on 2 June 2016.

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce OJ L 215, 25.8.2000.

Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under

Directive 95/46/EC of the European Parliament and of the Council. OJ L 39, 12.2.2010.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Foreign law

Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime. Washington, 3 October 2019.

Congress.gov. "H.R.7308 - 95th Congress (1977-1978): Foreign Intelligence Surveillance Act." September 7, 1978.

Congress.gov “H.R.4718 - 99th Congress (1985-1986): Computer Fraud and Abuse Act of 1986." October 16, 1986.

Congress.gov. "H.R.2048 - 114th Congress (2015-2016): USA FREEDOM Act of 2015." June 2, 2015.

Congress.gov. "Text - H.R.5040 - 115th Congress (2017-2018): Export Control Reform Act of 2018." April 17, 2018.

Right to Financial Privacy Act of 1978, RFPA; codified at 12 U.S.C. ch. 35, §3401.

Executive Order 12333 of December 4, 1981, establishing United States intelligence guidelines.

Presidential Policy Directive of January 17, 2014, on Signals Intelligence Activities.

Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§2701–2712)

Other Documents

Communication to the European Parliament and the Council of 27 November 2013, COM(2013) 846 final, 'Rebuilding Trust in EU-US Data Flows'.

Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, public consultation, 12 November 2020.

Draft Commission Implementing Decision published on 19 February 2021 pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.

European Commission, 2016. "Guide to the EU-US Privacy Shield".

European Data Protection Board. 2020. "EDPS Statement Following the Court of Justice Ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ('Schrems II') | European Data Protection Supervisor." July 17, 2020.

———. 2021a. "Census 2021: Portuguese DPA (CNPD) Suspended Data Flows to the USA | European Data Protection Board." April 28, 2021.

———. 2021b. "Transnational Codes of Conduct: Ensuring Consistency and Data Subject Rights through Co-Regulation." Linkedin. May 21, 2021.

Frequently Asked Questions of the European Data Protection Board of 23 July 2020 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

Guidelines 2/2018 of the European Data Protection Board of 25 May 2018 on derogations of Article 49 under Regulation 2016/679.

Information Commissioner's Office website. 2021. "Immigration Exemption." ICO. January 5, 2021.

Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross, 10 August 2020.

Letter of the European Data Protection Board to the European Parliament of 15 June 2020 regarding the agreement between the UK and the US on Access to Electronic Data for the Purpose of Countering Serious Crime.

Opinion of Advocate General Bot delivered on 23 September 2015, Maximillian Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:627

Opinion of the Court of 26 July 2017, Accord PNR UE-Canada, Avis 1/15, ECLI:EU:C:2016:656.

Opinion of the European Data Protection Supervisor 03/21 of 22 February 2021 on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement.

Recommendations 01/2020 of the European Data Protection Board adopted on 10 November 2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

Case-law

Judgment of the Court of 14 May 1974, J. Nold, Kohlen- und Baustoffgroßhandlung v Ruhrkohle Aktiengesellschaft, C-4/73, ECLI:EU:C:1974:51.

Judgment of the Court of 18 July 2013, European Commission and Others v Yassin Abdullah Kadi, C-584/10 P, ECLI:EU:C:2013:518.

Judgment of the Court of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others, C-293/12, ECLI:EU:C:2014:238.

Judgment of the Court of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650

Judgment of the Court of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, C-203/15, ECLI:EU:C:2016:970.

Judgment of the Court of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559

Judgment of the Court of 6 October 2020, La Quadrature du Net and Others v Premier ministre and Other, C-511/18, ECLI:EU:C:2020:791

Big Brother Watch and others v. United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15) [2018] ECHR 722.

United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018).

Sitography

www.anonos.com

www.dataembassy.com

www.wikipedia.it

www.wired.com