The third country problem under the GDPR: enhancing protection of data transfers with technology

Bjørn Aslak Juliussen *, Elisavet Kozyri **, Dag Johansen *** and Jon Petter Rui ****

Key Points

- Transfers of personal data from the protected area to third countries have been a continuous saga in the European Commission and the Court of Justice of the European Union (CJEU).
- The article analyses recent developments related to transfers of personal data to third countries, including shortcomings in the current transfer mechanisms.
- The role of technology as a safeguard in third-country transfers under the GDPR is then analysed under the different transfer mechanisms.
- The main contribution of this article is to link an analysis of the legal requirements for transfers of personal data to third countries with a computer science-based analysis of Privacy-Enhancing Technologies (PETs) in order to better ensure the overall proportionality, efficiency, and foreseeability in cross-border transfers of personal data to third countries.

Introduction

The overall objective of the General Data Protection Regulation (GDPR)[1] is two-fold: To contribute to the protection of privacy and personal data and to promote the free flow of personal data within the protected area[2] through uniform regulations and homogenized interpretations of those regulations.[3]

If a controller or processor in the protected area (the exporter) transfers personal data to a country, region, or international organization outside the EEA, the exporter gets the advantage of the free flow of personal data to an area without homogenized data protection rules and interpretations. Under such circumstances, it is imperative to establish requirements that contribute to the initial objective of the GDPR, the protection of privacy and personal data. In EU data protection law, this requirement is known as the 'essentially equivalent' requirement.[4] If personal data are to be transferred outside the protected area, the receiving country must have a level of personal data protection 'essentially equivalent' to the protected area.

The Court of Justice of the European Union (CJEU) concluded in both the Schrems I[5] and the Schrems II judgement[6] that US surveillance laws, which allow for general and indiscriminate surveillance, rendered the US data protection regime not 'essentially equivalent' to EU

* Bjørn Aslak Juliussen, Department of Computer Science, UiT The Arctic University of Norway, Tromsø, Norway. Email: bjorn.a.juliussen@uit.no
** Elisavet Kozyri, Department of Computer Science, UiT The Arctic University of Norway, Tromsø, Norway.
*** Dag Johansen, Department of Computer Science, UiT The Arctic University of Norway, Tromsø, Norway.
**** Jon Petter Rui, Faculty of Law, University of Bergen, Norway; Faculty of Law, UiT The Arctic University of Norway, Tromsø, Norway.
We thank the members of the Cyber Security Group and the Research Group on Crime Control and Security Law at UiT The Arctic University of Norway for helpful discussions.

1 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) OJ 2016 L 119/1.

2 The member states of the European Union (EU) and the three member states of the European Economic Area (EEA).

3 Regulation (EU) 2016/679 art 1.

4 Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* ECLI:EU:C:2020:559 (Grand Chamber) at para 105.

5 Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650 (Grand Chamber).

6 Case C-311/18.

data protection law. In the Schrems II judgement, the Court adjudged that the Privacy Shield[7] decision for the adequacy of the US personal data protection was inadequate and invalid.[8] The judgement gave exporters of personal data in the Union that transferred personal data to the US two alternatives: to discontinue the EU–US transfers or base the transfers on another legal basis.[9] The Schrems II judgement illustrates the complexity of international transfers of personal data to third countries in an ever-changing world. Similar situations altering the risks related to transfers of personal data could also happen due to unforeseeable or unavoidable events such as war or sudden regime changes in a third country.[10] The Schrems II judgment also serves as an illustration of the institutional tensions between the Commission and the CJEU. In order to negotiate international transfer agreements successfully, the Commission is compelled to engage in compromises. However, the CJEU, as a guardian of fundamental rights, adheres to a principle-based approach and rejects political compromises that would lead to violations of the fundamental right to the protection of personal data.[11]

In the modern digital landscape, many of the actors, including social media platforms, Internet service providers, and e-commerce sites, operate globally with a multi-jurisdictional presence. Thus, personal data collection, storage, and analysis have an international and non-territorial nature. Furthermore, modern cloud infrastructure includes backup solutions in multiple data centres across the globe to ensure fault tolerance in service delivery.[12] The non-territorial presence of service providers, as well as continuous backup computations across data centres, necessitates transfers of personal data across jurisdictions and continents. Both the economic value in personal data transfers and continuous backup computations illustrate that a full stop in international transfers due to a changing situation in a receiving third country is improbable.

After the Schrems II judgement, an alternative for exporters of personal data that based the transfer to the USA on the Privacy Shield decision was to base the transfer on another legal basis in Chapter V of the GDPR. Under such an alternate legal basis, the 2021 Standard Contractual Clause Decision,[13] the exporter has to assess the risk(s) concerning data protection compliance relating to the rules and regulations in the receiving third country. Such a process could be described as both unforeseeable for the exporter and with the potential to not provide efficient personal data protection. In a decision from May 2023, the Irish Data Protection Commission (DPC) concluded that the 2021 Standard Contractual Clauses (SCCs) decision could not compensate for the inadequate protection of personal data provided by US law for EU–US transfers conducted by Meta, formerly known as Facebook.[14] Meta Platforms Ireland Limited was thus imposed a 1.2 billion Euro fine by the Irish DPC for incompliance with Chapter V of the GDPR when transferring data from the protected area to the USA.

The announcement by the Commission and US authorities of a new framework for EU–US transfers has been presented as mitigating the legal uncertainty after the Schrems II judgement for EU–US transfers.[15] The EU–US Data Privacy Framework has resulted in an executive order from the US President ordering changes to US surveillance practices from 2022.[16] The Commission's proposal is expected to result in a new US adequacy decision.[17] The European Parliament has, however, called on the Commission to continue negotiations with the USA and not adopt adequacy based on the framework in a non-binding resolution.[18]

7 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–US Privacy Shield OJ 2016 L 207/1.

8 Case C-311/18 at para 184.

9 European Parliament, 'At a glance The CJEU judgement in the Schrems II case' (2020) <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf> accessed 13 July 2023.

10 Norwegian Data Protection Authority, Transfers of personal data to Russia and Ukraine. <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/overforing-av-data-til-russland-og-ukraina/> accessed 13 July 2023.

11 See further, Christopher Kuner, 'Op-ED: «International Data Transfers after Five Years of the GDPR: Postmodern Anxieties' available on EU Law Live: <https://eulawlive.com/op-ed-international-data-transfers-after-five-years-of-the-gdpr-postmodern-anxieties-by-christopher-kuner/> accessed 13 July 2023.

12 Jennifer Daskal, 'The Un-Territoriality of Data' (2014) 125(2) Yale Law Journal 326.

13 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 OJ 2021 L 199/31.

14 Data Protection Commission, DPC Inquiry Reference: IN-20-8-1. <https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf> accessed 13 July 2023.

15 European Commission, 'European Commission and the United States Joint Statement on Trans-Atlantic Data Privacy Framework 2022' <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087> accessed 13 July 2023.

16 The White House, 'Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities' <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/> accessed 13 July 2023.

17 See, European Commission, 'Draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework' 13 December 2022 <https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf> accessed 13 July 2023.

18 European Parliament Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU–US Data Privacy Framework (2023/2501(RSP)).

The article's main contribution is to link the findings from a legal analysis of the function and content of the 'essentially equivalent' requirement with a computer science-based analysis of privacy-enhancing technologies (PETs) in third-country transfers. The legal challenges with transfers to third countries are identified and analysed from a technical point of view to discuss whether technology could mitigate legal deficiencies in third-country transfers.

The motivation for analysing the interrelation between legal requirements and PETs is mainly due to the CJEU's invalidation of two different transfer tools after 2015.[19] One hypothesis is that bolstering cross-border transfers with technology enhancing the integrity and confidentiality of the (personal) data transferred would provide better data protection than contractual safeguards and procedural risk assessments, and contribute to the proportionality, efficiency, and foreseeability of cross-border transfers.[20] The article's main research questions are the following:

- What is the content and function of the requirement for 'essentially equivalent' protection in transfers to third countries? How is the 'essentially equivalent' requirement implemented in adequacy decisions and Standard Contractual Clauses?
- Whether and to what extent could PETs operationalize the requirement for 'essentially equivalent' data protection in transfers to third countries?

Legal requirements for cross-border transfers

Introduction to the different transfer mechanisms

The transfer concept is not defined in the GDPR. The European Data Protection Board (EDPB) has identified three cumulative criteria in the definition of transfers:

(i) A controller or processor is subject to the GDPR for the processing in question (the exporter).

(ii) The exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor which is importing the data (the importer).

(iii) The importer is located in a third country or is an international organization, irrespective of whether or not the importer is subject to the GDPR under Article 3.[21]

Transfers of personal data from the protected area and to third countries are prohibited under Article 44 GDPR as a general rule, with three exemptions. The rationale behind the general prohibition of transfers is to avoid the regulation being circumvented through transfers of personal data to third countries acting as 'personal data protection havens'.[22]

Chapter V of the GDPR establishes three exemptions from the general prohibition of cross-border transfers to third countries in Article 44.[23] These are that (i) transfers out of the protected area may be based on an adequacy decision from the European Commission (EC) stating that the third country has an adequate level of personal data protection; (ii) the transfer may be based on appropriate safeguards on a contractual level between the exporter and the importer pursuant to Article 46 GDPR. One such contractual safeguard is Standard Contractual Clauses (SCCs) adopted by the Commission under Article 46 (2) litra (C)[24]; and that (iii) the transfer may be based derogations on a case-by-case basis according to Article 49 GDPR.[25] Derogations may be employed exclusively as a transfer mechanism when the transfer of personal data is occasional and non-

19 See, Case C-362/14 (n 5) and Case C-311/18 (n 4).

20 The legal–technological interconnection in cross-border transfers has been suggested both by the EDPB: See, Recommendations 01/2020 on measures that supplement transfers tools to ensure compliance with the EU level of protection of personal data available: <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> accessed 13 July 2023 and by the European Commission, see Annex II of 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 OJ 2021 L 199/31.

21 EDPB, Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. <https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf> accessed 13 July 2023. The guidelines are based on the Judgement in the case C-101/01 *Bodil Lindqvist* ECR 1-12971 ECLI:EU:C:2003:596.

22 See, Recital 101 of Regulation (EU) 2016/769. The concept of personal data protection havens is like a tax haven, only for data protection. See further, Reuben Daniel Binns, David Millard and Lisa Harris, 'Data Havens, or Privacy sans Frontiéres: A Study of International Personal Data Transfers' (2014) *Websco'14: Proceedings of the 2014 ACM conference on Web science* 273 <https://doi.org/10.1145/2615569.2615650> accessed 13 July 2023.

23 It is presupposed that the personal data is lawfully collected and processed prior to the transfer.

24 The focus in the remainder of the article will be on SCCs and not the other appropriate safeguards in art 46, on account of SCCs being the predominantly used transfer mechanism.

25 The article will not analyse art 49 as a transfer tool due to its application on a specific case-by-case basis.

repetitive.[26] The overall purpose of the different transfer mechanisms in Chapter V of the GDPR is to ensure that personal data protection in the third country is 'essentially equivalent' to the protected area.[27]

The function and content of the 'Essentially Equivalent' requirement

The function of the requirement for 'essentially equivalent' data protection in the receiving third country is to ensure the continuity of the Union's high level of personal data protection and to ensure that the GDPR is not undermined when data are transferred to third countries.[28] The essentially equivalent requirement is established by reference to the GDPR read in light of the Charter of Fundamental Rights of the European Union,[29] and is a requirement regardless of the transfer tool applied.[30]

In the assessment of whether a third country offers 'essentially equivalent' protection, the situation differs somewhat depending on whether the transfer is based on an adequacy decision or appropriate safeguards under Article 46 GDPR.[31]

Standard contractual clauses and essentially equivalent protection

A decision adopted by the Commission pursuant to Article 46(2)(C) GDPR 'standard data protection clauses', has a general character and does not refer to a specific third country. Prior to the Schrems II judgement[32] exporters of personal data could, in essence, rely solely on the Standard Contractual Clauses adopted by the Commission prior to a third-country transfer. In the Schrems II judgment, the Court held that it is the exporters' responsibility to not export personal data to a country without essentially equivalent protection.[33] The Schrems II judgement could be described as altering the nature of SCCs from being a guarantee the exporters could rely on, to being a potential step to essentially equivalent personal data protection in the third country.

Depending on the prevailing situation in the receiving third country, the exporter should assess the risk of the transfer not meeting the 'essentially equivalent' requirement also when SCCs is the chosen transfer mechanism. According to Recital 19 of the new SCC decision adopted by the Commission,[34] personal data must not be transferred if the laws and practices of the third country of destination prevent the data importer from complying with the clauses. When assessing the rules and practices of the receiving third country, the exporter should take into account the content and nature and duration of the transfer, the type of recipient, the purpose of the processing, the laws, and practices of the receiving country, and any relevant contractual, technical or organizational measures applying to the transfer.[35] Such an assessment should be made in a Transfer Impact Assessment (TIA).[36] If the transfer risks not meeting the essentially equivalent requirement, the exporters should introduce additional measures to safeguard the transfer.

The assessment of when the transfer, due to the implementation of additional measures, does provide 'essentially equivalent' protection would vary based on the specifics of each transfer. The answer to whether personal data protection is 'essentially equivalent' would depend on the identified risk of data protection infringements in the third country due to the laws and practices and whether the contractual, organizational, and technical measures would mitigate the identified risks.[37] In case such additional measures do not make the situation in the receiving third country 'essentially equivalent', the transfer cannot lawfully be made.[38] If the exporters transfer personal data to third countries where the third country's authorities could access the data in a manner not 'essentially equivalent' to the GDPR, the exporters can risk fines of up to 20 million EUR or 4 per cent of global turnover, under Article 83(5)(C) GDPR.

In the section 'The role of PETs in third country transfers', various PETs are analysed to examine whether they could contribute to 'essentially equivalent' protection in transfers based on SCCs.

Adequacy decisions and essentially equivalent protection

The Commission's assessment of adequacy

An adequacy decision is an ex ante risk assessment of a specific third country where the Commission has

26 See further, recital 111-112 of Regulation (EU) 2016/679.

27 See, Case C-311/18 (n 4), at para 105.

28 Opinion from Advocate General Saugmandsgaard Øe in Case C-311/18 ECLI:EU:C:2019:1145 at para 117.

29 Case C-311/18 (n 4), at paras 99–100.

30 Ibid, at para 95.

31 For instance, Standard Contractual Clauses under Regulation (EU) 2016/679 art 46(2)(C).

32 Case C-311/18 (n 4).

33 Ibid.

34 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 OJ 2021 L 199/31.

35 Ibid, Recital 20.

36 Ibid, Recital 14.

37 Marcelo Corrales Compagnucci and others, 'Supplementary Measures and Appropriate Safeguards for International Transfers of Personal Data after Schrems II' (23 February 2022) p 23. <http://dx.doi.org/10.2139/ssrn.4042000> accessed 13 July 2023.

38 Case C-311/18 (n 4), at para 133.

assessed the adequacy of a specific third country's data protection based on the rule of law, respect for human rights, general and sectoral legislation, data protection rules, practices, case law and commitments, and means of redress in the third country.[39] An adequacy decision allows for transfers of personal data to pre-approved third countries without any authorization or approval.[40]

An adequacy decision does not require an identical level of personal data protection in the third country as in the protected area.[41] The level of protection in the third country may differ from the protected area as long as they prove that the system as a whole through the substance of privacy rights and their effective implementation, supervision, and enforcement delivers an essentially equivalent level of data protection.[42]

Future potential for inadequate adequacy

The European Commission is tasked under Article 45(2) GDPR to evaluate whether a third country offers essentially equivalent protection in adequacy decisions. The binding nature of such a decision could be invalidated by the CJEU only and not by national supervisory authorities.[43] The CJEU has invalidated adequacy decisions in both the Schrems I and II judgements.[44]

As a result of the Schrems II judgement, the European Commission announced a new EU–US Privacy framework on 25 March 2022.[45] On 7 October 2022, US President Joe Biden issued an Executive order with changes to US law regarding signal intelligence activities.[46]

EU law requires national laws that collect and retain personal data for national security purposes to be limited to what is strictly necessary.[47] In line with the consistent body of case law from the CJEU, with exception of cases established under urgency, access to retained personal data must be subject to a prior review carried out by a court or independent body whose decision is designed to limit access to what is strictly necessary to the objective pursued.[48] According to the US executive order Section 2(ii)(A), bulk collection of personal data transferred to the US could only be authorized when 'it is determined to be *necessary* to engage in bulk collection in order to advance a validated intelligence priority … '. The Executive Order thus has a requirement of necessity rather than the requirement of strict necessity established by the consistent body of CJEU case law.[49] Another important aspect in the Executive order is that it requires surveillance practices to be proportionate. The structured proportionality test conducted by the CJEU under EU law is, however, not part of the US constitutional doctrine.[50] A mere call for proportionality could therefore not amend disproportionate US surveillance practices. If the EU–US Data Privacy Framework results in an adopted adequacy decision from the Commission, it is therefore a potential for future inadequate adequacy to be established by the CJEU.

The CJEU has as of 2023, only assessed Adequacy Decisions regarding EU–US transfers.[51] Israel has an adequacy decision and similar surveillance practices as the USA.[52] After analysing surveillance laws and practices in Israeli law, Professor Douwe Korff concludes that the Israeli privacy regulations do not provide 'essentially equivalent' protection for EU data subjects.[53] A similar legal assessment has been made for the Adequacy Decision regarding Japan.[54] This legal assessment suggests that if these Adequacy Decisions are to be put

39 See, Regulation (EU) 2016/679 art 45(2) (a–c).

40 Regulation (EU) 2016/679 art 45(1) in fine.

41 Case C-362/14 (n 5), at para 73.

42 See for instance, Commission Implementing Decision (EU) 2022/254 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act OJ 2022 L 44/1.

43 See, art 288 of the Consolidated version of the Treaty of the Functioning of the European Union OJ 2012 C 326/47 and Case C-311/18 (n 4), at para 118.

44 It is an important aspect to have in mind that both these invalidations are caused by the effort of one individual, Maximillian Schrems, and not Data Protection Authorities or enforcement from Supervisory Authorities. See further, Kuner (n 11).

45 European Commission, 'European Commission and United States Joint Statement' (n 15).

46 White House (n 16).

47 See, Case C-311/18 (n 4) at para 176, Opinion 1/15 *EU–Canada PNR Agreement* ECLI:EU:C:2017:592 (Grand Chamber) at paras 140–41; Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790 (Grand Chamber) at para 67 and Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v premier ministre and Others* ECLI:EU:C:2020:791 (Grand Chamber) at para 130; Joined Cases C-793/19 and C-794/19 *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH* ECLI:EU:C:2022:702 (Grand Chamber).

48 Opinion 1/15 *EU–Canada PNR Agreement* ECLI:EU:C:2017:592 (Grand Chamber) at para 202; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* ECLI:EU:C:2016:970 (Grand Chamber) at para 120 and Case C-817/19 *Ligue des droits humains v Conseil des ministres* ECLI:EU:C:2022:491 (Grand Chamber) at para 115.

49 See n 47.

50 See Vicki C Jackson, 'Constitutional Law in an Age of Proportionality' (2014) 124 Yale Law Journal 394 and Kuner (n 11).

51 See, Case C-362/14 (n 5) and Case C-311/18 (n 4).

52 BBC, Pegasus scandal: Are we all becoming unknowing spies? <https://www.bbc.com/news/technology-57910355> accessed 13 July 2023.

53 Douwe Korff, 'Opinion on the Future of Personal Data Transfers from the EU/EEA to Israel and the Occupied Territories' <https://www.ianbrown.tech/2022/02/23/israels-privacy-protection-act-amendments-and-eu-adequacy/> accessed 13 July 2023.

54 Ana Gascón Marcén, 'The New Personal Data Protection in Japan: Is It Enough' in Micky Lee and Peichi Chung (eds), *Media Technologies for Work and Play in East Asia: Critical Perspectives on Japan and the Two Koreas* (Bristol, 2021; online edn, Policy Press Scholarship Online, 20 January 2022) <https://doi.org/10.1332/policypress/9781529213362.003.0006> accessed 13 July 2023.

under the scrutiny of the CJEU, there are indications that it might lead to invalidations.

The combination of a pragmatic Commission and the principle-based CJEU in the two Schrems judgements indicates that there is a risk that CJEU, in the future, will conclude that the EU–US transfer mechanism could be regarded as inadequate. In case other adequacy decisions are put under the test in the CJEU, it is also an inherent risk that these decisions will experience a comparable result as in the Schrems judgements. Such a resultant uncertainty necessitates exploration of technical measures to secure the protection of personal data transferred to third countries, even if such a transfer is based on an adequacy decision.

Disproportionate, ineffective, and unforeseeable transfer mechanisms?

The current state of affairs relating to cross-border transfers of personal data to third countries could be described as disproportionate, ineffective, and unforeseeable. Disproportionate because the CJEU has, in two separate judgements, concluded that the US law and practice does not provide essentially equivalent data protection. In spite of these invalidations of the main transfer mechanism, transfers to the US are not completely discontinued after the Schrems II judgement but mainly based on another legal basis.[55] A legal basis that, in the case of EU–US transfers conducted by Meta Platforms, Inc., led to a 1.2 billion Euro fine.[56]

The current state could be characterized as ineffective because exporters of personal data approach the challenging problem of transfers to third countries through complex risk assessments of the laws and practices in the receiving third country when relying on SCCs as the transfer mechanism. These Transfer Impact Assessments could be described as both tedious and procedural for the exporters. Our supposition is that they might lead to 'paper' compliance, but not necessarily to improved data protection in the receiving third country.

Lastly, the current state of affairs could be described as unforeseeable for the exporters due to the changing nature of the rules, requirements, and recommendations relating to transfers of personal data out of the protected area.

Adequacy decisions and appropriate safeguards, read in the light of the interpretation of the CJEU, require the GDPR and the rights in the Charter to be 'essentially' implemented in a third country, either through diplomatic negotiations between the Commission and the third country or as a contract between the exporter and importer. Regarding the first alternative, it is unlikely that a third country with a different legal culture, legal system, and fundamental rights instruments would implement data protection rights in a manner 'essentially' equivalent to the level within the protected area. Regarding the latter, a contract between private parties could not bind third-country governmental access to transferred personal data.

In the following sections, attention is therefore drawn to whether (PETs) could safeguard the confidentiality and protection of personal data transferred to third countries and thereby provide for a more effective alternative in third-country transfers.

The role of PETs in third-country transfers

Introduction

PETs are not defined in the GDPR. The European Union Agency for Cybersecurity (ENISA) defines PETs as a broad range of technologies that are designed for supporting privacy and data protection.[57]

An exporter of personal data relying on standard contractual clauses could be required, according to the SCC decision, to take both organizational and technical measures to ensure that a transfer to a third country is compliant with GDPR Chapter V interpreted in line with the Charter.[58] Various PETs that have potential as such technical measures are discussed in the following sections.

Currently, technology could represent potential additional measures that the exporter of personal data could introduce in order to comply with the 'essentially equivalent' requirement. PETs could also have the potential to make GDPR compliance more effective; they can enforce key principles of data protection. Thus, a data-transfer agreement could indicate the use of a pre-approved set of technologies to be employed by both parties for protecting the personal data transferred, instead of being a lengthy, complicated set of different modules of contractual clauses.

55 See n 4.

56 Data Protection Commission, DPC Inquiry Reference: IN-20-8-1. <https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf> accessed 13 July 2023.

57 ENISA, 'Privacy Enhancing Technologies (2022)' <https://www.enisa.europa.eu/news/enisa-news/promoting-data-protection-by-design-exploring-techniques> accessed 13 July 2023.

58 See, Annex II to 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 OJ 2021 L 199/31.

This section presents technical measures that can enforce different principles of data processing: integrity and confidentiality, purpose limitation, data minimization, accuracy, and informational self-determination.[59]

For each presented technical measure, we discuss the concept and applicability of the solution in cross-border transfers to third countries. Every technical solution that protects personal data imposes restrictions on how this data are used and processed, decreasing the data utility for the controller or processor. So, for each presented solution, we also discuss the trade-off between the degree of utility that is offered to the processor and the degree of data protection offered to the data subject.

Lastly, we discuss the legal status of the transfer if the different technical measures are applied. The measures have the potential to either:

- Render the processing outside the material scope of the transfer rules in Chapter V and thus also out of the scope of the regulation on the importers' hands; or
- Provide essentially equivalent data protection in the receiving third country; or
- Secure the processing, however, not to an extent that alters the legal status of the transfer.

The section concludes with some general comments on the analysed technical measures in terms of the overall proportionality, efficiency, and foreseeability the application of the measures could offer.

PETs with potential to leave the transfer outside the scope of chapter V

Before discussing different technical measures that might contribute to protecting personal data in cross-border transfers to third countries, it is important to define the scope of the regulation in relation to personal and non-personal data. These two legal concepts are important to discuss because they are relevant in the assessment of whether technical measures in the form of PETs render the transfer outside the scope of the transfer rules in Chapter V of the GDPR.

The GDPR and the principles of data protection apply to personal data, ie information relating to an identified or identifiable natural person.[60] When personal data are anonymized, the link between the natural person and the data no longer exists. The GDPR and the principles of data protection do therefore not apply to anonymous information and if personal data is rendered anonymous in such a manner that natural persons are not or no longer identifiable from the data, the processing is left outside the scope of the GDPR and is regarded as non-personal data.[61]

When determining whether data is regarded as personal or non-personal and under or outside of the scope of the GDPR, the key element is an assessment of identifiability. To determine whether a natural person is still identifiable, an account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify a natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify a natural person, account should be taken of all objective factors, such as the cost of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and the technological developments.[62]

However, there is a non-settled scholarly debate and a divergence in the legal sources on the question of whether the GDPR regulates identifiability in an absolute or relative manner.[63] Under the absolute manner of assessing identifiability, no risk of reidentifications is accepted. If there is a mere theoretical risk that someone somewhere could reverse-engineer the process and identify a natural person, the data should be regarded as personal data.[64] The relative approach, on the other hand, accepts a theoretical risk of reidentification. The risk of reidentification is considered from the objective factors mentioned in Recital 26 GDPR in order to answer whether the data are regarded as personal data under the scope of the regulation or non-personal data outside the scope.

A recent judgement of April 2023 from the Eighth Chamber of the General Court regarding the concept of personal data in Regulation (EU) 2018/1725[65] might

59 See, Regulation (EU) 2016/679 art 5.

60 See, Regulation (EU) 2016/679 art 4(1) and Recital 26 of Regulation (EU) 2016/679.

61 See, Regulation (EU) 2016/679 Recital 26.

62 Ibid.

63 Gerald Spindler and Philipp Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7(2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 163 and Emily M Weitzenboeck and others, 'The GDPR and Unstructured Data: Is Anonymization Possible?' (2022) 12(3) International Data Privacy Law 184 <https://doi.org/10.1093/idpl/ipac008> accessed 13 July 2023.

64 See, WP29, Opinion 04/2014 on Anonymization Techniques. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 13 July 2023.

65 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC OJ 2018 L 295/39.

shed some light on the concept of personal data also under the GDPR.[66] The disputed question, in essence, concerned whether sharing an alphanumeric code, related to an identifiable natural person, should be considered anonymous or pseudonymous data in the hand of the recipient when the information allowing re-identification was not shared. The General Court interpreted the definition of personal data in Regulation (EU) 2018/1725, which corresponds to the definition under the GDPR, in line with the Breyer judgement. The General Court does not provide a clear general answer to the question of whether information that can only be used to identify a specific individual when additional information, not possessed by the entity, is available, can be considered as personal data. However, the General Court concludes that the actual risk of reidentification must be assessed and that sharing of pseudonymous data where the repository necessary for identification is not shared does not automatically renders the data either anonymous or pseudonymous on the receiver's hand. The judgement of the General Court is in line with the relative manner of assessing identifiability.

In the Judgement, data were shared but not transferred to a third country. Furthermore, the Judgement concerned Regulation 2018/1725 and not the GDPR. The Judgement of the General Court therefore has relevance but needs to be applied with some caution in relation to third-country transfers. Related to the third country problem, the judgement is relevant for the following scenario: The data transferred is identifiable for the exporter, but the exported data are processed in a manner where identifying natural persons requires information kept by the exporter in the protected area. The GDPR assesses the status of data, whether it is regarded as personal data or anonymized data, after the identifiability assessment. We argue that the identifiability assessment, in such a situation, is different depending on whether the exporter or importer is holding the data. We argue that, from the perspective of the importer in the third country holding the data, the relative manner of assessing identifiability in the GDPR could leave the transfer of data processed by the use of technical measures outside the scope of the transfer rules in Chapter V of the GDPR because the data are no longer linked to a natural person in the receiving third country without access to information kept by the exporter.

In a situation where technical measures are applied to render the transfer outside the scope of the transfer rules in Chapter V of the GDPR the following elaboration is important to make: the processing of personal data in the protected area is, unquestionably, under the scope of the GDPR. When the technical safeguards are applied to the personal data by the exporter in the protected area prior to the export and identifiability of a natural person is not possible, the transfer may fall outside the scope of the transfer rules in Chapter V. The rationale behind this statement is that the definition of transfers from the EDPB is not fulfilled for such a processing operation. Point two of the definition of the EDPB is not fulfilled in such a scenario because the data made available for the importer does not fulfil the definition of personal data. An important disclaimer is that technical measures must be implemented on the personal data before the point of export. The objective of the transfer rules is to protect data subjects in the protected area from disproportionate data protection rules in a third-country jurisdiction. In a situation where the data transferred is not personal data, this purpose becomes inapplicable. The further reasoning behind why different PETs may cause the transfer to fall outside the transfer rules in Chapter V is elaborated under each of the sections analysing the different PETs.

Pseudonymization as a technical safeguard in transfers to third countries

Pseudonymization protects personal data by replacing the identifier between information in a data set and a natural person.[67] Personal identifiers, for instance, a name, age, or an identification number, are replaced by a pseudonym, for instance, a random number or a hash, and the link between the identifier and the pseudonym is protected by keeping the additional information needed to identify the natural person separately and subject to technical and organizational safeguards.[68]

In relation to cross-border transfers to third countries, the applicability of pseudonymization could be illustrated by the use of an example. Suppose that a patient, an EU data subject, is employed with a wearable sensor that monitors blood pressure and heart rate. The wearable device sends data to servers in a third country for analysis before the result is reported to the patient's doctor. The doctor needs to link the results from the analysis with the identity of the patient. However, the

66 Case T-557/20 *Single Resolution Board (SRB) v European Data Protection Supervisor* ECLI:EU:T:2023:219 General Court (Eighth Chamber, Extended Composition).

67 Pseudonymization is defined under art 4(5) in Regulation (EU) 2016/679 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'.

68 European Union Agency for Cybersecurity, 'Deploying Pseudonymization Techniques (2022)' <https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques> accessed 13 July 2023.

identity of the patient is not necessary to perform the analysis of the patient's data in the third country. Pseudonymization could be applied to replace the name of the patient with a pseudonym, for instance, a number or a random hash. The number of random hash is transferred together with the sensor data to the third country. The analysis of the sensor data is performed and transferred back to the protected area. The linking between the result of the analysis and the identity of the natural person behind the pseudonym is then performed in the protected area.

The example above illustrates that pseudonymization could be applied to enhance the confidentiality of personal data and limit the identifiability of natural persons and thus contribute to the principle of data minimization in third-country transfer. To what extent could the pseudonymization of natural persons' identifiers offer confidentiality protection? The level of confidentiality protection could also be illustrated with an example. Suppose that an online service provider in the protected area stores the following data from its users: time-stamp with the users' time zone, IP address, type, and version of browser, set and preferences of natural languages in the browser settings, and the operating system of the user's computer. The IP address is pseudonymized and kept in a repository by the controller or processor.

Now, suppose that the controller and processor wish to transfer the stored data to a third country for further storage in a cloud. Is the pseudonymization of the IP address sufficient to protect the data subject from re-identification attempts in the third country? The Panopticlick experiment has shown that even though the IP address is pseudonymized, information on time-zone, language settings, type and version of the browser, and the operating system is sufficient to identify a browser and thus also a specific data subject.[69]

Unlike anonymization, pseudonymization is not a technique that renders the processing outside the material scope of the GDPR by default. Personal data that have undergone pseudonymization is still defined as personal data and pseudonymization is an example of an appropriate safeguard under Article 6(4)(e), data protection by design and by default under Article 25, and as a security measure under Article 32.

The recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data from the EDPB,[70] also regard pseudonymization as an additional measure for essentially equivalent protection and not a measure that renders the processing on the importer's hand outside the scope of the GDPR. The EDPB concludes that pseudonymization might represent a relevant additional measure for cross-border transfers to third countries. The conclusion from the EDPB is relevant for pseudonymization techniques that fulfil the following requirements: (i) the personal data can no longer be attributed to a specific data subject or used to single out the data subject in a larger group, (ii) the additional information necessary to identify the data subject is held exclusively by the exporter, (iii) disclosure or unauthorized use of the additional information is prevented by technical and organizational safeguards and (iv) the exporter has thoroughly analysed the data in question and taken into account any information that the authorities in the recipient third country may possess that the pseudonymized personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information.[71]

The recommendations from the EDPB call for the exporter to take into account 'any information the authorities in the receiving third country may possess' when considering whether pseudonymization is an efficient additional measure to secure personal data in a transfer to a third country.

The recommendations on pseudonymization as an additional safeguard in transfer to third countries from the EDPB and the definition of pseudonymization in Article 4(5) GDPR are somewhat different. While the definition in Article 4(5) presupposes that only information kept separately by the controller or processors should be assessed when evaluating whether natural persons are identifiable.[72] Recommendation 01/2020 presupposes that the exporter of personal data should also assess the risk of indirect identification from information kept by third-country authorities when applying pseudonymization as a technical safeguard in transfers to third countries.

To conclude on the legal status of pseudonymization as a technical measure to safeguard transfers, the transfer of pseudonymized data may either contribute to essentially equivalent protection dependent on the specifics of the transfers such as the sensitivity of the

69 Electronic Frontier Foundation, Cover your tracks. <https://coveryourtracks.eff.org/> accessed 13 July 2023.

70 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data page 23 (2020). <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> accessed 13 July 2023.

71 Ibid.

72 See the wording provided '*that such additional information is kept separately and is subject to technical and organisational measures*' in art 4(5) of Regulation (EU) 2016/679 and WP29, Opinion 05/14 on Anonymization Techniques (2014) p 10 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 13 July 2023.

personal data and the laws and practices in the receiving third country.[73] In such a situation, the analysis of laws and practices in the receiving third country is necessary. Therefore, as an overall conclusion, pseudonymization as a technical measure would contribute to securing the transfers, but not alter the legal status of the transfers by default.

Sovereignty cloud models: moving the cloud servers to the protected area

The overall concept in sovereign cloud models is that the physical infrastructures necessitating third-country transfers, such as servers, are moved from third countries to the protected area in the EEA. In a sovereign cloud environment, personal data reside in the protected area under the GDPR, making the requirements for transfer to third countries excessive. Sovereign cloud models are therefore a technique applied to not transfer data out of the protected area.[74]

Several exporters of personal data are exploring sovereign cloud models. For instance, Microsoft announced the launch of Microsoft Cloud for Sovereignty in July 2022.[75] The new cloud solution is offered to public sector customers that need to guarantee that personal data are only processed in a given region, for instance in the protected area. Other technology companies have announced comparable products to mitigate the risk related to transferring personal data to third countries. For instance, Google's sovereign control for Workspace products is such a service.[76]

The various sovereign cloud solutions incorporate different techniques to enforce personal data protection and confidentiality, including encryption and access controls. Nevertheless, the overall concept underlying such cloud infrastructures is to maintain the data within the jurisdictional boundaries of one specific geographical location. Consequently, the various sovereign cloud providers contend that they offer a solution where the transfer rules in Chapter V become inapplicable because the data are not transferred to a third country.[77]

The following paragraphs will discuss a legal issue when a controller or processor established in the Union makes use of a sovereign cloud solution: how should a controller or processor in the protected area assess the situation where personal data are processed on a sovereign cloud in the protected area and the cloud provider is registered in a third country or is an EU subsidiary of an enterprise registered in a third country?

To recapitulate, the GDPR does not define transfers out of the protected area. A common definition of such transfers is given in guidelines from the EDPB.[78] In the situation where personal data are stored and processed in the protected area but the cloud provider is an enterprise registered in a third country, the situation is not regarded as a transfer under the EDPB's guidelines.[79]

In the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), cross-border transfers to third countries are defined as a process where the data are transferred to a recipient that is subject to the jurisdiction of a State that is not a party to Convention 108+.[80] The definition of transfers in Convention 108+ is further elaborated in the Draft Explanatory Report to the Convention.[81] In the explanatory report, transborder data transfers are further explained as a process where 'personal data are disclosed or made available to a recipient subject to the jurisdiction of another State or international organisation'.[82] A transborder transfer under Convention 108+ would therefore cover also situations where personal data are made available to a jurisdiction of a non-party to the convention without the personal data being imported to the non-party state. Such a situation could occur when making personal data available on a cloud, even though the cloud server infrastructure is physically located in a state that is party to the Convention.[83]

Convention 108+ is an instrument of European data protection law as promulgated by the Council of Europe (CoE) and is closely linked to the right to data protection under Article 8 of the European Convention of Human Rights. Convention 108+ does therefore have relevance

73 See, Regulation (EU) 2016/679 Recital 26.

74 Microsoft Corporation, 'Microsoft Cloud for Sovereignty: The most Flexible and Comprehensive Solution for Digital Sovereignty (2022)' <https://www.microsoft.com/en-us/industry/sovereignty/cloud> accessed 13 July 2023.

75 Ibid.

76 Google, 'Advancing Digital Sovereignty on Europe's Terms' <https://cloud.google.com/blog/products/identity-security/advancing-digital-sovereignty-on-europes-terms> accessed 13 July 2023.

77 Microsoft Corporation (n 74).

78 EDPB, 'Guidelines 05/2021 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR' <https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf> accessed 13 July 2023.

79 Ibid.

80 Council of Europe, 'Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+) Article 14, 18.05.2018' <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> accessed 13 July 2023.

81 Draft Explanatory Report—Convention 108 Modernised. <https://rm.coe.int/convention-for-the-protection-of-individuals-with-regard-to-automatic-/16806b6ec2> accessed 13 July 2023.

82 Ibid.

83 See also, Cécil de Terwagne, 'Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data' (2021) 40 Computer Law and Security Review 105497 <https://doi.org/10.1016/j.clsr.2020.105497> accessed 13 July 2023.

for the interpretation of the right to privacy and data protection in the Charter.[84] Neither the GDPR nor the Convention has an explicit collision rule.[85] However, the GDPR does not define transfers. The definition is based on a recommendation from the EDPB that is based on a judgement from the CJEU under the predecessor of the GDPR.[86] The definition of transfers in Convention 108+ Article 14 could therefore represent a valid factor in the interpretation of a transfer in EU data protection law. This conclusion has to be elucidated. In Opinion of the Court 2/13, the CJEU concluded that the EU legal order constituted a distinct legal order and that the draft agreement regarding the EU accession to the ECHR was liable to affect the specific characteristics of EU law and its autonomy.[87] Consequently, the relationship between EU law and CoE law could be described as one marked by a certain tension. However, in May 2023, the CoE and the European Commission published a revised agreement on the EU accession to the ECHR.[88] The purpose of the revised agreement is to alleviate the concerns raised by the CJEU in opinion 2/13 regarding the autonomy of EU law. This recent development would, most likely, facilitate the future accession of the EU to the ECHR, and therefore also underscoring the relevance of Convention 108+ within the domain of EU data protection law.

In a German judgement from the Administrative Court in Wiesbaden from December 2021, the Court interpreted a situation similar to when a sovereign cloud is controlled by a third-country enterprise. The German Court concluded that even though the personal data never left the protected area under the GDPR, the situation could be defined as a transfer if the company processing the personal data is under the jurisdiction of a third country.[89] The German administrative court did not assess the guidelines on transfers from the EDPB and the Court's view does therefore not represent a homogeneously European interpretation of the GDPR.

The question of whether processing personal data in the protected area by a processor under the jurisdiction of a third country could be regarded as a transfer is also the subject of a non-settled scholarly debate.[90]

The question was adjudged by the French Conseil d'Etat in March 2021. Unlike the German Administrative Court, the French Court concluded that a platform processing personal data where the processing took place in the protected area by a Dutch subsidiary of a US corporation did not constitute a transfer of personal data to a third country.[91] However, the Conseil d'Etat still assessed the risk of US authorities accessing personal data processed on the platform. The risk-based approach pursued by the Conseil d'Etat could entail that it is not that significant whether the situation is defined as a transfer to a third country or not since the Court assessed the risks of US authorities getting access to the personal data even after concluding that the processing was not defined as a transfer.

In the situation where the data reside in a sovereign cloud in Europe, but the cloud is controlled by a third-country enterprise or a subsidiary of a third-country enterprise, several legal sources call for an assessment of the risks related to a potential non-authorized access to the personal data in the cloud by third-country authorities. In such a risk-based approach to the processing, relevant factors include both the nature of the personal data, the purpose of the processing, and technical safeguards, for instance, encryption and logs on data access.[92]

To conclude on the legal status of sovereign clouds in relation to transfers to third countries, a sovereign cloud solution is a technical measure with the potential to render the processing outside of the scope of the transfer rules in Chapter V of the GDPR if the cloud service

84 See, The Charter art 52(3).

85 Jorg Ukrow, 'Data Protection without Frontiers: On the Relationship between EU GDPR and Amended CoE Convention' (2018) 4 European Data Protection Law Review 239. The only reference to the CoE convention is in recital 105 of the GDPR which refers to Convention 108 and not Convention 108+.

86 An interpretation of transfers was last adjudged by the CJEU in the Lindqvist judgement from 2003 under the predecessor of the GDPR. The CJEU concluded in the judgement that uploading personal data to a website under the jurisdiction of a third country was not regarded as a transfer under Directive 95/46.

87 Opinion 2/13 of the Court ECLI:EU:C:2014:2454 (Full Court) at para 200.

88 Council of Europe, Latest meeting of the CDDH ad hoc negotiation Group '46 + 1' <https://rm.coe.int/report-to-the-cddh/1680aa9816> accessed 13 July 2023.

89 IAPP, 'New EU Data Blockage as German Court would Ban many Cookie Management Providers' <https://iapp.org/news/a/new-eu-data-blockage-as-german-court-would-ban-many-cookie-management-providers/> accessed 13 July 2023.

90 See, for instance, Laura Drechsler, 'Defining Personal Data Transfers for the Context of the General Data Protection Regulation: A Critical Perspective on the Guidelines 5/2021 of the European Data Protection Board' (2022) 10(1) Privacy in Germany 24; Laura Drechsler and Irene Kamara, 'Essential Equivalence as a Benchmark for International Data Transfers After Schrems II' in Eleni Kosta and Ronald Leenes (eds), *Research Handbook on EU data protection* (Edward Elgar Publishing Ltd, 2022). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881875> accessed 13 July 2023 and Svetlana Yakovleva, 'GDPR Transfer Rules vs Rules on Territorial Scope: A Critical Reflection on Recent EDPB Guidelines from both EU and International Trade Law Perspectives' *European Law Blog* (9 December 2021). <https://europeanlawblog.eu/2021/12/09/gdpr-transfer-rules-vs-rules-on-territorial-scope-a-critical-reflection-on-recent-edpb-guidelines-from-both-eu-and-international-trade-law-perspectives/> accessed 13 July 2023.

91 National Free Software and others CE N 444937. <https://www.conseil-etat.fr/content/download/157044/document/444937%20-%20CNLL%20et%20autres.pdf> accessed 13 July 2023.

92 See, Regulation (EU) 2016/679 arts 6(4)(e) and 32(1)(a).

provider is a company registered in the EEA. Both the legal status of the cloud in relation to the transfer rules and the risk of unauthorized access to personal data by authorities from third countries would depend on the nationality and jurisdiction of the cloud provider.

Data encryption

An example of a technical safeguard mentioned in the GDPR is data encryption.[93] Encryption can be applied to enforce the confidentiality of the personal data, by making the data readable only to authorized principals. Encryption is one of the most widely used security measurements deployed by computer systems.

When users interact with their e-banking account or official governmental websites, or when sending messages, encryption is almost always used to protect the confidentiality of the users' data.

Although encryption is widely adopted, there are certain assumptions that one needs to make when using it. These assumptions impact the level of data protection, the level of data utility, and the level of additional measures necessary in order to reach 'essentially equivalent' data protection if personal data are transferred outside the protected area. To be more specific, let us first give an overview of symmetric encryption.

This encryption procedure takes as input the piece of information to be protected, known as the plaintext, and a secret value, known as the secret key, and it returns a randomly looking sequence of bits, known as the ciphertext. The only efficient way in which the ciphertext can be converted back to the original plaintext is by invoking the corresponding decryption procedure with that ciphertext and that secret key. So, only those principals that know the secret key can decrypt the ciphertext. Consequently, encryption obscures the sensitive information for all principals but those that know the secret key. Figure 1 depicts the procedure described above.

The confidentiality protection that is provided by encryption is relative to principals that know the secret key since anyone that knows the key can always retrieve the sensitive information from the ciphertext. We consider two scenarios that differ in the assumption of who knows the secret key, and how this assumption influences the level of protection, utility, and the legal status of the cross-border transfer to a third country. For what follows, consider a user (ie data subject) in the protected area providing personal data to a processor in the Union (ie data exporter), which in turn makes the data accessible to a web service (ie data importer) based in a third country. The personal data are encrypted in its entirety

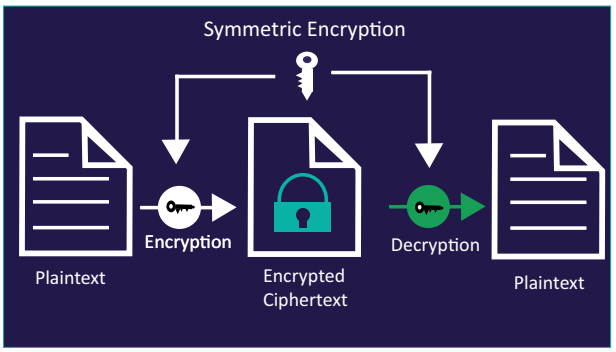

Figure 1: Illustration of symmetric encryption.

with a secret key, both for its transfer to the web service and for its storage within that web service.

(i) **User-side encryption.** Assume that only the user knows the secret key. This entails that only the users can efficiently retrieve their personal data from the ciphertext; their personal data is not revealed to the exporter within the protected area or the importer in the third country. This technical solution provides high confidentiality protection. However, the high confidentiality protection comes at the cost of the low utility for both the exporter and importer of personal data. Here, the exporter and the web service access only the ciphertext and thus no useful processing can be applied to this obscured data, except for storing or forwarding it. Thus, this technical solution might be appropriate for web services that provide encrypted and robust cloud storage or peer-to-peer communication.

(ii) **Server-side encryption.** Assume the data subject, the exporter, and the web service importing the personal data in the third country know the secret key. This means that only these three parties can efficiently retrieve the user's personal data. Specifically, adversaries that eavesdrop on the network communication between the data subject and the exporter or between the exporter and the importer in the third country might access the transferred ciphertexts, but cannot efficiently retrieve the encrypted sensitive data. So, server-side encryption ensures that the user's personal data are only shared with the exporter and the importer and no one else, but it imposes no restrictions on how the web service utilizes that data. This implies that the data utility is high for the web service.

Regarding the principles of data protection, user-side and server-side encryption implicate different principles.

93 Ibid.

Both techniques, to some extent, enhance the confidentiality of personal data by making the data only readable to authorized principals. However, user-side encryption limits the potential for the processor of personal data to process it, strengthening both the principles of data minimization and purpose limitation.

The two main different encryption techniques we described above, user-side and server-side encryption are met in real applications. Consider WhatsApp, a popular messaging application. WhatsApp offers end-to-end encryption between the communicating parties.[94] This means that these parties encrypt the messages they exchange using a secret key only known to them. So, any personal information included in these messages is accessible only by the communicating parties, and no one else, including WhatsApp. This approach is closer to scenario (i) discussed above. The metadata of the communication, though, seems to be accessible to WhatsApp. This messaging service might know the parties that communicated when they communicated, and for how long. Metadata can be applied to identify an individual natural person and would therefore be included in the definition of personal data under GDPR Article 4(1) depending on the specifics of the case under question. So, if this metadata is subject to GDPR, then additional measurements need to be taken for its protection in cross-border transfers.

WhatsApp might be required by a third-country authority to terminate end-to-end encryption for users within the third country and share collected information with the authorities of the third country. This approach would be closer to scenario (ii). Specifically, Brazil intends to demand that WhatsApp support traceability[95] for the exchanged messages, recording who communicate what and when. Such an intention is directly opposite to both the principle of data minimization, storage limitation, confidentiality, and proportionality in the GDPR. In the case where a Brazilian citizen is communicating with an EU citizen, the answer to the question of how WhatsApp will resolve the contradictory data protection requirements remains.

Consider now Gmail, the email application of Google. Here, emails are encrypted by a secret key that is known by both the user (ie client-side) and Gmail (ie server-side).[96] So, this approach is closer to scenario (ii). Now, assume that an EU data subject sends an email containing sensitive personal data to a US user. This email will be ultimately stored on a US server. How is Gmail going to resolve the conflicting protection requirements between those that govern the EU-sent email and the US-stored data?

These two real-life examples illustrate that if the secret key is accessible by the data importer in the third country of destination, encryption as an additional measure under the SCC decision could potentially represent a false sense of data protection, and server-side encryption would not be sufficient as an additional measure to reach 'essentially equivalent' protection is such situations.

The question of whether client-side encryption, where only the user accesses the secret key, as the first example above, is considered personal data under the GDPR is open for debate. As a starting point, encryption is regarded as a measure for secure processing under Article 32 GDPR and not an anonymization technique. Encrypted data are, therefore, regarded as personal data under the GDPR.

We argue that if personal data are encrypted before the point of export and the secret key is held in the protected area inaccessible to the importer in a receiving third country and if the encryption protocol is so strong that there is no means reasonably likely to be used to reverse the encrypted data back to personal data, the transfer is rendered outside the transfer rules in Chapter V.[97]

The decryption process in the protected area is still regarded as personal data processing. However, the transfer of the user-side encrypted data is not regarded as the transfer of personal data under the risk-based approach in Recital 26 because the importer cannot identify a natural person from the ciphertext alone.[98] This understanding of user-side encryption and the scope of the transfer rules in Chapter V of the GDPR only applies if the encryption takes place prior to the point of export.

The conclusion on the legal status of encryption in relation to cross-border transfers of personal data is, therefore, different for user-side and server-side encryption. User-side encryption has the potential to derive the

94 WhatsApp, 'About End-to-end Encryption' (2022) <https://faq.whatsapp.com/791574747982248/?locale=en_US> accessed 13 July 2023.

95 Ibid.

96 Google, 'Email Encryption in Transit' <https://support.google.com/mail/answer/6330403?hl=en> accessed 13 July 2023.

97 See also, W Kuan Hon, Christopher Millard and Ian Walden, 'The Problem of Personal Data in Cloud Computing: What Information is Regulated? —the Cloud of Unknowing' (2011) 1(4) International Data Privacy Law 211, <https://doi.org/10.1093/idpl/ipr018> accessed 13 July 2023.

98 In the Safe Harbour agreement, the European Commission considered the transfer of uses-side encrypted data to the US as not an export of personal data if the secret key was not transferred together with the data. The CJEU did not challenge this notion under the invalidation in the Schrems I judgement. See, 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 2000 L 215/7.

transfer of encrypted data to a third country outside the scope of the transfer rules in Chapter V of the GDPR.

Server-side encryption offers lower confidentiality protection, compared to user-side encryption. This means that the controller or processor exporting the personal data to the web service in the third country might need to take additional measures to ensure full GDPR compliance if the exporter is relying on SCC as a transfer tool and there are identified risks related to the laws and practices of the receiving third country.

Notice that, under server-side encryption, if the web service is subject to laws and practices under the jurisdiction of a third country that might require the acquisition of secret keys, then the user's personal data are potentially accessible by the third country authorities, too. Across different jurisdictions, there are several examples of existing legislation that calls for encryption methods to implement mandatory backdoors that can access the encrypted ciphertext. One example of such anti-encryption legislation is the Australian Telecommunications and Other Legislation Amendment (Assistance and Access Act) from 2018.[99] The amendment to the act requires telecommunications providers and other providers of server-side encryption to give technical assistance, including providing encryption keys, to Australian law enforcement agencies upon request. Another example is the non-binding call from the European Council in the Resolution on Encryption.[100] These examples, and the current legislative trend of requiring access to secret keys for law enforcement and intelligence gathering purposes has the consequence that the effect of server-side encryption as a technical measure in third-country transfer might give a false sense of confidentiality protection for the personal data transferred.

Depending on the laws of the third country, one might therefore need to relax the assumption of who knows the secret key to include the authorities of the third country, further lowering the confidentiality protection and raising the risk relating to the transfer of personal server-side encrypted data. User-side encryption does not suffer from the problem relating to authority acquisition of secret keys.

The final conclusion of the legal status of transferring encrypted data out of the protected area is that user-side encryption may render the transfer outside the scope of the transfer rules in Chapter V and that server-side encryption, dependent on the law and practices in the third country, could be a potential first step in complying with the essentially equivalent requirement.

Homomorphic encryption

Ideally, a technological solution would offer both high confidentiality protection for a user's personal data and high utility for the data processor. Homomorphic encryption (HE) has been proposed as a tool that approximates this ideal. Under HE, personal data can be encrypted with a secret key that only the user knows—obtaining protection benefits highlighted in (i)—and the data processor can perform certain computations on the encrypted information (apart from storing or forwarding)—obtaining utility benefits highlighted in (ii). Specifically, the characteristic property of HE is as follows: applying a certain operation on some homomorphically encrypted data and then decrypting the result with the corresponding secret key, yields a plaintext that equals the result of directly applying that operation to the original data. So, under HE, users encrypt their personal data, send the ciphertext to a third party, have the party apply certain computations to the ciphertext, receive and decrypt the processed ciphertext, and then access the plaintext, which is equal to the result of directly applying that computation to their original data. Figure 2 depicts this procedure.

We now give an example where HE could be an applicable technical measure in relation to cross-border transfers to third countries. Consider a database that is maintained by a service in a third country and that is homomorphically encrypted with a secret key known only by a data subject in the protected area. Assume that the employed HE scheme can preserve search operations, meaning that applying a homomorphically encrypted search query on the homomorphically encrypted database returns the same result as if that query was applied directly to the original database. The EU data subject can then issue a query, which might contain personal information, to the database in the third country, without having this service learn the content of the database, the issued query, and the result of the query.

However, HE is not ideal. There is a trade-off between the complexity of the computation that can be applied to the ciphertexts and the computational performance that can be achieved. The higher the

99 See further, Peter Alexander Earls Davis, 'Decrypting Australia's "Anti-Encryption" Legislation: The Meaning and Effect of the "systemic weakness" Limitation' (2022) 44 Computer Law and Security Review <https://doi.org/10.1016/j.clsr.2022.105659> accessed 13 July 2023.

100 Council of the European Union, Council Resolution on Encryption-Security through encryption and security despite encryption. 13084/1/20 REV 1. <https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf> accessed 13 July 2023.

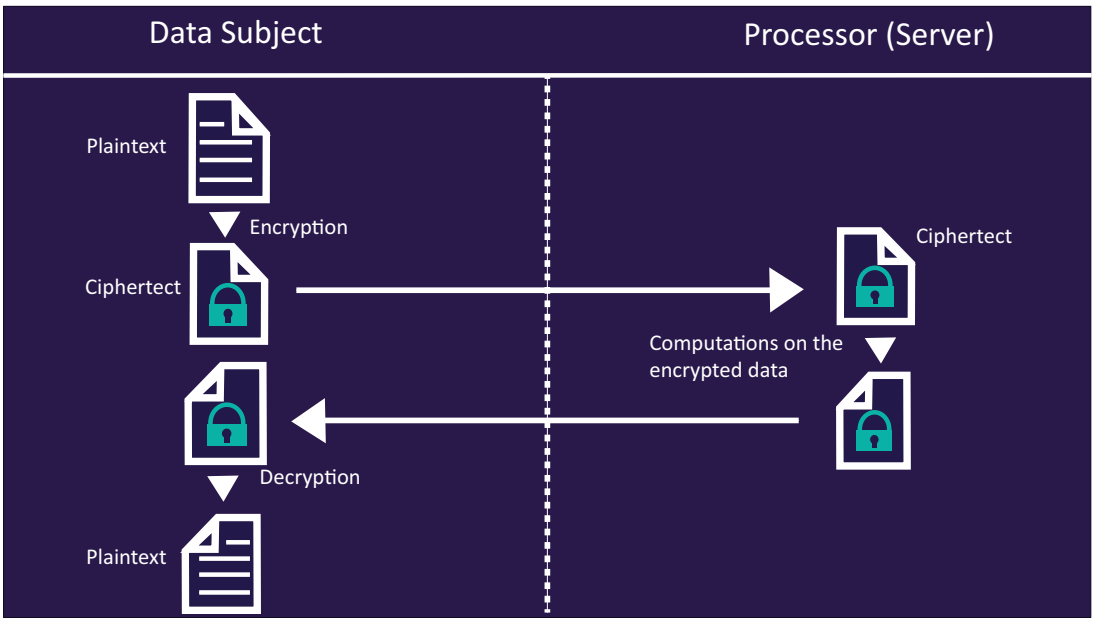

Figure 2: Illustration of homomorphic encryption.

complexity of the computation that one needs to apply to ciphertexts, the slower this computation becomes (compared to applying the same computation to plaintext), rendering HE impractical for general purpose processing.[101] Although improving the performance of HE for a wider spectrum of computation is an active field of research.[102]

Employing HE to enforce the data protection principles of confidentiality and purpose limitation in cross-border transfers to third countries could be a sensible proposal, as many other authors have already argued.[103] HE could be regarded as equivalent to original user-side encryption, for purposes of GDPR compliance in transfer to third countries.

Could the application of HE render the transfer outside the scope of the transfer rules in Chapter V from the perspective of the importer in the third country?

We suggest a new approach when assessing the legal status of homomorphic encryption as a safeguard in transfers to third countries. If personal data are encrypted by the data subject itself, or by a data exporter in the protected area, and the encryption key is not controlled or accessible by the data importer in the third country, good reasons call for interpreting the situation on the left side of Figure 2, prior to the point of export, as the processing of personal data (encryption) and processing of pseudonymized data (decryption) and the situation on the right side of Figure 2 (processing in the third country) as the processing of non-personal data. In such an interpretation, the processing in the third country is left outside of the material scope of the transfer rules in Chapter V. The interpretation builds on the following considerations: (i) the secret key is not accessible to the importer of personal data and (ii) it is not computationally efficient to reverse-engineer the personal data from the computations on the encrypted data in the third country.

Trusted execution environments

A trusted execution environment (TEE) allows data to be processed without ever being accessed by unauthorized parties. Compared to homomorphic encryption, arbitrary computation can be practically applied to these data, while its confidentiality is still protected.

Compared to the other solutions discussed in this article, a TEE is a hardware solution. An example of TEE is Intel's SGX processor. Here, data are stored encrypted

101 Furkan Turan, Sujoy Sinha Roy and Ingrid Verbauwhede, 'HEAWS: An Accelerator for Homomorphic Encryption on the Amazon AWS FPGA' (2020) 69(8) IEEE Transactions on Computers 1185 <https://doi.org/10.1109/TC.2020.2988765> accessed 13 July 2023.

102 Vinod Vaikuntanathan, 'Computing Blindfolded: New Developments in Fully Homomorphic Encryption' (2011) in proceedings of the IEEE 52nd Annual Symposium on Foundations of Computer Science 5 <https://doi.org/10.1109/FOCS.2011.98> accessed 13 July 2023.

103 See, Compagnucci and others (n 37) 23.; Marcelo Corrales Compagnucci and others, 'Homomorphic Encryption: The Holy Grail for Big Data Analytics and Legal Compliance in the Pharmaceutical and Healthcare Sector?' (2019) 3 European Pharmaceutical Law Review 144 <https://doi.org/10.21552/eplr/2019/4/5> accessed 13 July 2023 and Luigi Sgaglione and Giovanni Mazzeo, 'A GDPR-Compliant Approach to Real-Time Processing of Sensitive Data' in Giuseppe De Pietro and others (eds), *Intelligent Interactive Multimedia Systems and Services* (Springer, Cham 2019).

in an isolated memory space, called an enclave. When performing a computation, the processor fetches data from the enclave, decrypts this data, applies the computation, and stores the result encrypted back to the enclave. Consequently, no other process running on the same machine, not even the operating system, can access data in the enclave, unless it knows the corresponding secret key. So, a TEE can provide high confidentiality protection and high utility since arbitrary computations can be applied to sensitive data.

We now give a scenario where a TEE is being employed as part of transfers from the protected area to a third country. Consider a medical centre in the protected area in the EU or EEA and a company in the USA that specializes in a rare-disease diagnosis. This company has proprietary software that takes as input patient's data and outputs the likelihood that this patient suffers from the specific disease. This software is executed on a machine equipped with the SGX processor. The EU medical centre can then encrypt a patient's medical information with a key known by that processor, send the ciphertext to the company in the USA, and have it stored and processed within an SGX enclave. The encrypted result of the processing can then be sent back to the medical centre in the protected area, where it is being decrypted and examined.

So, in this scenario, a TEE solution offers confidentiality protection for the transfer of personal information from the protected area to a third country.

Except for the confidentiality of data, a TEE could also be used to enhance the right to redress, for instance the right to information, rectification, and erasure in the GDPR interpreted in light of Article 47 of the Charter. A TEE can be used to attest the code that it executes. For example, assume that the data exporter and data importer have agreed on using the transferred data only in a certain way. A TEE can then be used to securely capture a fingerprint (ie hash) of the code to be executed on this data, and send the fingerprint to the data exporter. The data exporter is then able to verify whether the fingerprint corresponds to the pre-agreed processing of data, and thus check whether the sent data are used in the expected way.

Would the application of a TEE in a cross-border transfer to a third country render the data transfer outside the scope of the transfer rules in Chapter V of the GDPR? To answer this question, we examine two issues. First, to employ a TEE, one needs to trust the provider of that TEE. For example, one needs to trust Intel that the SGX processor functions as it is supposed to and that the keys employed cannot be compromised or handed to third-country authorities. The discussion on the legal status of the TEE under this question is similar to the discussion on sovereign cloud models above. Secondly, researchers have exposed data leakages through timing side-channels, when SGX is employed.[104] If a TEE has been certified and is offered by a trusted European provider and if the timing side-channel leakages are not enough to reconstruct personal data, then the application of a TEE could render a data transfer outside the scope of the transfer rules in Chapter V of the GDPR, or at least, enforce the 'essentially equivalent' requirement of GDPR.

Federated learning

One of the reasons behind transferring data from the protected area to a third country is for this data to be used in the training of a machine learning (ML) model. There are cases where many different institutions, from possibly different countries, want to collaborate in the training of a ML model, but without revealing their training data, which consists of personal data, to the other participants.

To address this constraint, federated learning has been proposed. In federated learning, the participants share the model—not the raw training data. Each time, a participant receives the partially trained model from another participant, uses their training data to further train the model, and then sends the result to the next participant. This procedure continues until the resulting trained model satisfies some optimization criteria.

Employing federated learning offers high utility since the ML model is trained on the entire training data, even if these data are split among different participants.

It seems that federated learning offers higher confidentiality protection than sending raw data to third parties. However, it has been established that the partially trained model (ie values of certain parameters of the model) might still reveal information about the training data.[105]

Although, it is not clear whether this leaked information is enough to reconstruct personal data. In any case, one could conservatively deduce that dependent on the specifics of the transfer and the receiving third country,

104 Johannes Götzfried and others, 'Cache Attacks on Intel SGX' (2017) Proceedings of the 10th European Workshop on Systems Security 1 <https://doi.org/10.1145/3065913.3065915> accessed 13 July 2023.

105 David Enthoven and Zaid Al-Ars, 'Fidel: Reconstructing Private Training Samples from Weight Updates in Federated Learning' (2022) proceedings of the 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS) 1 <https://doi.org/10.1109/IOTSMS58070.2022.10062088> accessed 13 July 2023.

employing federating learning is not sufficient to comply with the 'essentially equivalent' requirement, and additional measures should be taken to protect personal data, especially if the training data are sensitive data, such as for instance health data under GDPR Article 9(1).

Using differential privacy

One way to increase confidentiality protection of federating learning is by slightly perturbing the partially trained model (ie the values of the parameters) such that information about the training data is not leaked to the model and the model is still precise enough. Differential privacy could achieve a perturbation with such properties.

Differential privacy is a technique that can be employed in any processing of data. Some processing of a dataset is said to be differentially private if the result of this processing does not depend too heavily on the individual data entries: by deleting a data entry, it is unlikely that the result of processing will change, too. Any data processing can become differentially private if certain noise is added to the result.

Federating learning is a special kind of data processing, and thus, researchers have developed differentially private federating learning (DPFL). In DPFL, the model is trained in a differentially private way. For example, whenever a participant updates the parameters of the model, a certain amount of noise is being added to their values, such that the resulting values do not depend too much on the individual training data items of that participant. DPFL has drawn the attention of many researchers and tech companies.[106]

The degree of confidentiality protection offered by DPFL increases when more noise is added during training. So, there is a point where personal data cannot be efficiently retrieved from the trained model, in which case one complies with the 'essentially equivalent' requirement and potentially also leaves the scope of the GDPR because the trained model could not be reversed back to personal data and is therefore no longer defined as personal data under Article 4(1) of the regulation interpreted in line with Recital 26.

At the same time, the addition of noise can harm utility. This is because adding too much noise might render the trained model useless; its precision might drop when used on new data entries.

Consequently, the challenge ahead is to be able to calculate the minimum amount of noise needed to be added to a partially trained model, such that the 'essentially equivalent' requirement is satisfied when transferring data to a third country.

Using secure multi-party computation

Another enforcement mechanism for confidentiality that is employed along federated learning is Secure Multi-Party Computation (MPC). Under MPC, several parties owing separate data, participate in the computation of a function on all these data, without explicitly sharing their own data with the other parties. For example, an MPC protocol can enable four participants to compute the minimum of their salaries, but without revealing to each other the salary that each participant receives. Such a protocol only involves message exchanges between the participants—it does not rely on any third trusted party for carrying out any computation. However, MPC does not necessarily protect the privacy of the participant's data. This is because the very result of the function that an MPC protocol computes might reveal information about personal data. In the example above, by the end of the MPC protocol, every participant learns that at least one of the participants gets the resulting minimum salary (ie information that some consider personal)—albeit they do not certainly know who.

In the specific case of federated learning, the participants can execute an MPC protocol to compute an aggregation function on their individual partially trained models. The result of the aggregation would be the final trained model. But similar to the example above, the final model might reveal information about individual partially trained models, and possibly, the corresponding training data sets.

Given that MPC alone does not guarantee the protection of private training data, it cannot be used as a basis for satisfying the 'essentially equivalent' requirement in cross-border transfers to third countries.

Data tracing and informational self-determination

EU data protection law and the GDPR build on a notion of informational self-determination.[107] Informational self-determination represents the rationale behind the right of information for the data subject in Article 13, the right to access in Article 15, rectification in Article 16, and erasure in Article 17. The right to informational self-determination is also related to the right to redress

106 ICO, 'Chapter 5: Privacy Enhancing Technologies (PETs)' <https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf> accessed 13 July 2023.

107 See, for instance, Regulation (EU) 2016/679 Recitals 32, 50, 59, 63, and 66.

in Article 47 of the Charter of fundamental rights of the European Union.[108]

However, the rights of the data subjects in the mentioned Articles would only represent theoretical and illusory rights—and not practical and enforceable rights—if it is impossible to trace where the personal data are stored in a system. The importance of knowing where data flow in a system and where pieces of information with the potential to identify natural persons are transferred is especially present in third-country transfers.

In this section, we discuss whether new technologies, such as data tracing or provenance logs, might represent a solution to strengthen data subjects' right to informational self-determination within the rights to information, access, rectification, and erasure of personal data in the GDPR in cross-border transfers to third countries.[109]

The rights of data subjects under the GDPR are supposed to travel with the personal data of EU and EEA data subjects if and when personal data are transferred outside the protected area.[110] Data tracing can provide the technical means for implementing this requirement. Here, a piece of data are associated with a label. This label follows the associated data wherever it goes. For example, when data are copied from one storage location to another or when it is sent through the network to another physical location, the associated label follows the data to the new location. Also, when data are used as input to a computation, then the associated label is propagated to the result of this computation. This is because information about this input data is likely encoded in the result, and thus, the associated label owes to follow that information, too.

A label can encode any information that is relevant for the given application. For instance, a label can record the origin of the associated data or even its detailed provenance, including the processing steps the associated data have passed through and the different locations it has traversed. A label could include restrictions on how the associated data are allowed to be used. In such a case, whenever an entity attempts to process a labelled piece of data, it would first have to check whether this processing adheres to the restrictions included in the label.

Tracing and provenance mechanisms have been studied and deployed on different abstraction levels in a system. Constructing and querying the provenance of data within a database has been extensively explored.[111] Tracing has also been implemented at the level of operating systems,[112] where one can reason about the provenance of files. Establishing end-to-end traceability for internet of things (IoT) application, from the sensors to the data-processing stage, to the user interface is a current research front.

The ability of data tracing to capture the origin of data and record it in the associated label can support the right to access and the right to erasure. For example, if labels include information about the owner of the original data, and a principal wants to have their data deleted, then an automatic process could search through the system and delete all the information that is associated with a label specifying that principal as the owner.

Having labels record the provenance of data can support the right to redress. This information could help the user understand how their data have been used and whether this use is in accordance with certain agreements. For example, provenance information could be used to check whether data processing in the third country obeys the safeguards agreed upon between the EU data exporter and the data importer in the receiving third country.

For tracing to be used as a means of enforcement of the GDPR, the employed tracing mechanism should be trusted. The entities that implement tracing within the computer systems in the third country should provide some assurance about the integrity of the tracing mechanism. Such assurance could be regulated by the legal safeguards agreed between the parties.

Notice that tracing alone does not offer confidentiality protection. Though it can be augmented with a monitoring mechanism that ensures data are read only by principals prescribed by use restrictions within the associated label. Also, tracing does not, by itself, impede the utility of data. Finally, it does impose computational, storage, and network overhead, since all these aspects should accommodate the additional information carried by the labels.

Conclusion

The different technical measures analysed in the sections above illustrate that the confidentiality of personal data and the right to redress in third-country transfers could be enhanced by the use of different technologies. How the different technical measures could alter the legal status of the transfers is represented in Table 1.

108 See, Recital 104 of Regulation (EU) 2016/679 and Case C-311/18 (n 4), at para 188.

109 See, arts 13, 15–17 in Regulation (EU) 2016/679.

110 See, Regulation (EU) 2016/679 art 44.

111 Faheem Zafar and others, 'Trustworthy Data: A Survey, Taxonomy and Future Trends of Secure Provenance Schemes' (2017) 94 Journal of Network and Computer Applications 50 <https://doi.org/10.1016/j.jnca.2017.06.003> accessed 13 July 2023.

112 Thomas Pasquier and others, 'Practical Whole-system Provenance Capture' in SoCC'17: Proceedings of the 2017 Symposium on Cloud Computing <https://doi.org/10.1145/3127479.3129249> accessed 13 July 2023.

Table 1: Summary of the legal status of the analysed PETs

	Outside the scope of Chapter V	Essentially equivalent	Secure processing
Pseudonymization			✓
Sovereign clouds	✓		
User-side encryption	✓		
Server-side encryption			✓
Homomorphic encryption	✓		
Trusted execution environments	✓		
Federated learning (FL)			✓
FL with differential privacy		✓	
FL with multi-party computation			✓
Data tracing		✓	

If a technical measure alters the legal status of a transfer on the importers' hands and renders the processing in the third country outside the scope of the regulation, this should not be understood as a legal technicality for GDPR compliance. The overall data protection of such a transfer is still in line with Union data protection law because the transferred data do not contain information possible to reverse back to an identifiable natural person.

However, as also stated in the analysis of the legal status under each technical measure, the measures do not automatically render the processing outside of the scope of Chapter V of the regulation. Such a result is dependent on the specifics of the technologies and the general classification in the table above is a simplification. The table above should be read as a summary and should also be read in line with the disclaimers made in the main text under each section above. A tick in a column in the table also implies ticks in the columns to the right. More research is needed to validate these claims. The legal status of these technical measures also needs to be periodically revaluated in light of new technological advancements.

The article illustrates the importance of critically analysing the role of technical measures as safeguards in transfers of personal data to third countries. By critically analysing how, for instance, server-side encryption does not necessarily protect personal data from disproportionate surveillance laws in third countries, it is possible to move forward in the ever-lasting problem of third-country transfers.

The introduction of technical measures could contribute to the overall efficiency of exporters in the protected area exporting personal data to third countries. Compared to analysing the laws and practices in the receiving third country, the introduction of technology reducing the amount of personal data being transferred or rendering the transfer outside the scope of the transfer rules could be a more sensible proposal. However, as the analysis of both server-side encryption and sovereign clouds illustrates it is sometimes necessary to both analyse the laws of the third country and the technical measures introduced.

The analysis of the technical measures has shown that technologies safeguarding the transfer may, in some cases, leave the processing after the point of export outside of the transfer rules in Chapter V. These measures may improve the foreseeability for exporters in the protected area and at the same time not compromise with the fundamental right to personal data protection because the data transferred could not be applied to reidentify a natural person.

Third-country transfers have been a continuous changing saga in EU data protection law. Different technical measures could contribute to the proportionality when transferring personal data out of the protected area, even to countries with disproportionate surveillance laws, by either not transferring data where natural persons are identifiable or by making access to personal data in the third country difficult.

Technical measures and Privacy Enhancing Technologies, therefore, have a role in third-country transfers. By introducing different technical safeguards to the transfer, the overall proportionality, efficiency, and foreseeability in transfers may be enhanced.

As both a general finding and a methodology for future work, the article illustrates the importance of working closely together in the interface between law and computer science to both properly get a clear and firm understanding of the facts the law should be applied on and to develop new technologies in compliance with fundamental rights, law, and regulations.

https://doi.org/10.1093/idpl/ipad013