EUI ROBERT SCHUMAN CENTRE

RSC 2025/07
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

WORKING PAPER

International Transfers of Personal V. Non-Personal Data: Reconstructing the EU Legal Puzzle

Natalia Menéndez González, Danielle Borges, Marco Botta

European University Institute
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

International Transfers of Personal V. Non-Personal Data: Reconstructing the EU Legal Puzzle

Natalia Menéndez González, Danielle Borges, Marco Botta

RSC Working Paper 2025/07

ISSN 1028-3625

Natalia Menéndez González, Danielle Borges, Marco Botta, 2025

Published in July 2025 by the European University Institute.

Badia Fiesolana, via dei Roccettini 9

I – 50014 San Domenico di Fiesole (FI)

Italy

Robert Schumann Centre for Advanced Studies
The Robert Schuman Centre for Advanced Studies, created in 1992 and currently directed by Professor Erik Jones, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics. The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

Centre for a Digital Society
The Centre for a Digital Society (CDS), created in 2022 and directed by Prof. Pier Luigi Parcu, analyses the challenges of digital transformation and its impact on markets and democracy. Within the EUI, the CDS is part of the Robert Schuman Centre for Advanced Studies. With its research, policy debates and executive training programmes, the CDS aims at advising policy makers on how to cope with the challenges generated by the digitalisation process. To do so, it adopts an inter-disciplinary approach relying on in-house expertise in law, economics and political sciences, and by actively cooper-ating with computer scientists and engineers from partner institutions.

For further information: https://digitalsociety.eui.eu

Abstract

Data has become an essential input in the digital economy: having access to a large, updated, accurate and verified source of data is a key competitive advantage, allowing a firm to personalize its services for its customers and engaging in targeted advertising. In addition, data access is increasingly important to train AI models. At the same time, data easily 'moves' across the borders, generating an exponential growth of cross-border data flows.

The paper analyses the EU data *acquis* – *i.e.* a complex regulatory framework developed by the European Union during the past years. The framework essentially pursues two distinct goals: on the one hand, it aims at fostering B2B data sharing, to enhance the competitiveness of the EU digital economy. On the other hand, via the adoption of the General Data Protection Regulation (GDPR) in 2016, the EU has also opted for a high level of protection for personal data. The paper discusses conflicts and overlaps between these two goals, looking at the case of international data transfers of 'personal' and 'non-personal' data. In this regard, the paper compares the legal framework applicable to international transfer of personal data under the GDPR, with the new legal framework concerning the transfer of non-personal data under the Data Act (DA) and the Data Governance Act (DGA).The paper argues that the blurring distinction between personal and non-personal data, the narrow interpretation of anonymization techniques, the expansion of the 'appropriate measures' requirements in the GDPR, and the introduction of new rules for the transfer of non-personal data have the effect of limiting the ability of economic operators to engage in data processing activities outside the EU and potentially limit international data transfers outside the EU.

Keywords

General Data Protection Regulation; international data transfer; personal v. non-personal data; data anonymization; Data Act; Data Governance Act; data protection

1. Introduction

Data is generally defined as the 'oil' of the 21st-century economy: companies that successfully collect and process large amounts of diversified and updated data manage to provide more personalised services to their customers, and they can engage in targeted advertising, thus becoming more competitive. Besides providing target services and advertising, data is also an essential input to train Large Language Models (LLMs); data is thus at the core of the development of generative AI. In other words, data access boosts productivity and innovation of every firm operating in the digital economy. Agriculture, health care and financial sector are some of the industries which have recorded a rapid increase in the use of data in the past years.1 Small and medium-sized enterprises (SMEs) especially benefit from enhanced access to data, reducing their costs and increasing their productivity.2

Due to economic value, data is also increasingly traded between private parties (i.e. business-2business, B2B, data sharing). In particular, data sharing often has a cross-border dimension: global business operations, cloud computing, and cross-border communications often imply international data transfers. According to estimates of the World Economic Forum, in 2022, international data flows contributed to $ 2.8 trillion to global GDP, a figure that has grown 45-fold over the last decade.[3] In a world increasingly digitized and hyper connected, economic growth is driven heavily by international data flows.

Though the value of the EU data economy has steadily risen over the past decade, it remains far less developed when compared to the US data market.[4] With the aim of establishing an internal market for data, in 2019 the European Commission has adopted a European Data Strategy,[5] and during the past years proposed several far-reaching pieces of data legislation aiming at fostering business-to-business (B2B) data sharing - i.e. the EU data *acquis*. First, the Data Governance Act (DGA) includes several provisions pointing at increasing trust in data intermediaries, thus incentivising the degree of B2B data sharing.[6] Secondly, the recently adopted Data Act (DA) incentivises the portability of personal and non-personal data generated by Internet of Things (IoT) devices.[7] In particular, the user may ask the device manufacturer to transfer the data collected and produced by product usage to a third party. Thirdly, the Digital Markets Act (DMA)[8] and the Digital Services Act (DSA)[9] include specific obligations, mandating large digital platforms to grant access to their dataset when specific conditions are fulfilled. The emerging EU data *acquis* also includes sector-specific regulations, mandating B2B data sharing in the chemical,[10] banking,[11] automotive,[12] electricity,[13] tele-

1 <https://www.mckinsey.com/mgi/overview/in-the-news/the-ascendancy-of-international-data-flows#> (last access 26.11.2024).
2 Ibid.
3 <https://www.weforum.org/stories/2023/01/data-flows-cross-border-wef23/> (last access 26.11.2024).
4 According to a 2020 EU Commission study, in 2019 the value of the EU data market was "approximately 2.5% smaller than that produced in the US." European Commission, The European Data Market Monitoring Tool. Published on 6.7.2020, p. 9. The report is available at: <https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-update> (last accessed 28.1.2025).
5 <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en> (last access 26.11.2024).
6 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). OJ L- 152/1, 3.6.2022
7 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). OJ L-2023/2854, 22.12.2023.
8 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector, amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). OJ L-265/1, 12.10.2022.
9 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)
10 Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December, 2006, concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94, as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC. OJ L-396/1, 30.12.2006.
11 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2 Directive). OJ L-337/35, 23.12.2015. Art. 36.
12 Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018, on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009, and repealing Directive 2007/46/EC. OJ L-151/1, 14.6.2018. Art. 61.
13 Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019, on common rules for the internal market for electricity and amending Directive 2012/27/EU. OJ L-158/125, 14.6.2019. Art. 23.

com,[14] and postal sectors.[15] Shortly, such pieces of legislation will also overlap with the data-sharing rules adopted within the Common European Data Spaces.[16] Following the publication of the Data Strategy in 2020, in fact, the European Commission has promoted the establishment of common Data Spaces in strategic fields, such as energy, health, mobility…[17] Within each Data Space, different stakeholders could pool data in a secure and privacy friendly environment, and be subject to clear data governance rules.

To sum up, the EU data *acquis* includes an extensive number of new legislations that share the common aim of fostering B2B data sharing, though the legislations have a different scope of application (i.e. horizontal v. sectoral) and they either introduce a favourable legal framework to incentivize data sharing, or they 'mandate' data sharing when specific conditions are fulfilled.

Besides fostering B2B data sharing, the EU data *acquis* has a second main goal: the protection of personal data, as a fundamental right within the EU legal system. The General Data Protection Regulation (GDPR),[18] adopted in 2016 and in force since May 2018, is one of the most advanced legislations in the world in terms of data protection. If the data is 'personal', it falls under the scope of the GDPR, and thus it could be shared between two parties only subject to the data subject's consent or if one of the legal bases under Art. 6 GDPR GDPR is fulfilled. In addition, Chapter 5 GDPR provides for stringent rules when personal data is 'exported' outside the European Union (i.e., international data transfer). While the GDPR rules on international data transfers have the legitimate purpose of ensuring that the recipient country provides a degree of protection "equivalent" to the EU standards, such rules negatively affect international data transfer and thus they could potentially hamper the degree of B2B data sharing. Finally, while the GDPR regime is applicable to international transfers of 'personal' data, the DGA and the DA provide for specific rules in relation to international transfers of 'non-personal' data, thus further complicating the applicable legal framework.

The paper attempts to 'reconstruct' the 'puzzle' represented by the emerging EU data *acquis,* which includes several legislations, either promoting data sharing or fostering the protection of personal data. In particular, the paper analyses the possible conflicts between these two goals, by analysing the EU legal regime concerning the transfer of data outside the EU. The distinction between personal and non-personal data and the concept of anonymized data is key to determine the scope of the GDPR application in the context of international data transfers, as well as the application of the DA and the DGA in the context of international transfers of non-personal data. A further sub-question discussed in the paper is whether and to what extent, in the context of the digital economy, personal data may be anonymized and thus become non-personal.

The paper builds upon the previous work of the authors analysing different aspects of the EU data *acquis*, such as the principle of fair, reasonable and non-discriminatory (FRAND) compensation in the context of B2B data sharing,[19] and at the relationship between the GDPR and the DMA in the contest of the prohibition of data combination and cross-use under Art. 5(2) DMA.[20]

While Section 2 discusses the distinction between personal and non-personal data, Sections 3 and 4 analyse the concept of data anonymization in the literature as well as under EU law. Finally, Sec-

14 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018, establishing the European Electronic Communications Code (EECC). OJ L-321/36, 17.12.2018. Art. 112.

15 Directive 2008/6/EC of the European Parliament and of the Council of 20 February 2008, amending Directive 97/67/EC with regard to the full accomplishment of the internal market of Community postal services. OJ L-52/3, 27.2.2008. Art. 11a.

16 European Commission Staff Working Document on Common European Data Spaces. Published in Brussels on 23.2.2022, SWD(2022)45 final. The document is available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces (last accessed 28.1.2025).

17 For further information about the Common European Data Spaces, see: https://digital-strategy.ec.europa.eu/en/policies/data-spaces (last accessed 28.1.2025).

18 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons about the processing of personal data, and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR). OJ L-119/1, 4.5.2016.

19 Marco Botta (2023), "The Scattered EU Acquis on B2B Data Sharing." 27(10) GRUR International: 917-918. arco Botta (2023), "The principle of FRAND in B2B data sharing: Lessons from licensing of standard essential patents and competition law remedies." Concurrences No 3-2023.

20 Marco Botta, Danielle Borges (2023), "User Consent at the Interface of the DMA and the GDPR. A Privacy-setting Solution to Ensure Compliance with ART. 5(2) DMA" RSCAS working paper 2023/68. The paper is available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4650373> (last access 4.9.2024).

tion 5 builds upon the previous sections, analysing the distinction between personal and non-personal data as well as data anonymization in the context of international data transfers, while Section 6 presents the conclusions.

2. Defining whether data is personal or non-personal

To verify whether a certain piece of data is personal or non-personal it is necessary to check if it is related to an identified or identifiable natural person.[21] Accordingly, there is data that is always non-personal since it is never related to an identified or identifiable natural person, such as weather information or stock prices. But there is also data that once was 'personal', but later it was rendered 'anonymous' in such a manner that the individual is no longer identifiable. This is called 'anonymised data', it is considered non-personal data and thus falls outside the scope of the GDPR, according to Recital 26.[22] On the other hand, when personal data undergoes pseudonymisation techniques, it is no longer possible to attribute this data to a specific natural person without the use of additional information.[23] According to Article 4(5) GDPR, 'pseudonymisation is 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 is not attributed to an identified or identifiable natural person.' In this sense, the European Data Protection Board (EDPB) further clarifies that the process of pseudonymisation consists of replacing directly identifying data, such as name, first name, personal number, and phone number, included in a dataset with indirectly identifying data (alias, sequential number, etc.). This replacement makes it possible to process the data of individuals without being able to identify them in a direct way. However, it is possible to trace the identity of these individuals thanks to the additional data.[24] According to the Article 29 Data Protection Working Party's[25] opinion on anonymisation techniques, pseudonymization is a helpful security tool but not an anonymization technique.[26] As such, pseudonymised data is still personal data and is subject to the scope of the GDPR. In this vein, it is possible to say that pseudonymisation is also reversible, unlike anonymisation, and for this reason, it falls within the scope of the GDPR.[27] This leads to the conclusion that data needs to pass the test established by Recital 26 GDPR to check whether they are pseudonymised or anonymised.

Fink and Pallas argue that the test provided by Recital 26 GDPR embraces a risk-based approach to qualify information. Accordingly, where there is a reasonable risk of identification of a person, data ought to be treated as personal data, and where that risk is merely negligent, data can be treated as non-personal data, and this is even though identification cannot be excluded with absolute cer-

21 Article 4(1) GDPR: ''personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

22 Recital 26 GDPR states that "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, 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 the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

23 Michele Finck and Frank Pallas (2020) They who must not be identified—distinguishing personal from non-personal data under the GDPR. International Data Privacy Law, 2020, Vol. 10, No. 1.

24 'Secure Personal Data | European Data Protection Board' <https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en> accessed 17 September 2024.

25 Article 29 Data Protection Working Party was set up under Article 29 of Directive 95/46/EC. It was an independent European advisory body on data protection and privacy. It was replaced by the European Data Protection Board effective on 25 May 2018 (entry into application of the GDPR).

26 Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques Adopted on 10 April 2014

27 See EDPB, 'Data Protection Guidelines for Small Business'. Available at https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en#:~:text=As%20such%2C%20pseudonymised%20data%20is,the%20processing%20_of%20_personal%20data (last access 4.9.2024)

tainty.[28]

The distinction between pseudonymised and anonymised data can sometimes be blurred, and therefore, it can be difficult to determine whether information constitutes personal data in certain situations. One of the aspects to look at in this regard is from whose perspective the likelihood of identification ought to be assessed. Under the absolute approach, all possibilities and chances in which the data controller would be able to identify the data subject individually are taken into account, even theoretical chances of combining data so that the individual is identifiable are included,[29] and only a real no-risk of re-identification is accepted.[30] On the other hand, under the 'relative' approach, only realistic chances of combining data in order to identify an individual are considered and not highly theoretical identification risks, and hence "the nature of data as personal depends on the means reasonably likely to be carried out by the data holder to re-identify data."[31] The wording of Recital 26 GDPR ('[t]o determine whether a natural person is identifiable, account should be taken of all the means reasonably *likely* [emphasis added] to be used') seems to be more in line with the relative approach. Although Recitals are not legally binding, it should be considered that courts often use them to interpret a particular provision of EU legislation, especially if multiple interpretations of a certain provision are possible. However, as we will see in the following section of this paper, the CJEU has not adopted a unitary position regarding this question.

3. Data Anonymization

The question of data anonymisation and the legal regime applied to such data is of enormous importance within the digital economy. The "anonymous" character of the data excludes them from the application of the personal data regime, mainly the GDPR. Considering the high level of protection that this regulation grants to personal data, from an industry point of view, the fact of being subject to its requirements entails a huge difference from a compliance perspective. Further, from a digital innovation perspective, the processing of non-personal data is much more interesting, since EU legislation allows the free movement of such data with some exceptions in the DA and DGA. However, considering our digital society, whether certain data is considered anonymous and therefore fall within a certain regulatory regime is not a straightforward question. Depending on whether one follows an absolute (all possibilities and chances for re-identification are taken into account) or relative (only realistic chances of re-identification are considered) approach, the conceptualization of specific data as anonymous or pseudonymous might change.

Following a growing number of scholars and relevant stakeholders,[32] as data processing technologies evolve and more data becomes accessible for processing, full anonymisation is no longer achievable. This means that the huge amount of data collected from different sources on different aspects of a person, even though individually considered would not allow her identification, once combined, they do. Article 29 Data Protection Working Party goes even as far as to claim that the danger of acceptable re-identification needs a near-zero probability, an idealistic and impractical condition that cannot be guaranteed in the Big Data era, after acknowledging the technological challenges and hazards inherent to anonymization.[33] Statistically speaking, even without moving within the realm of new technologies, research has shown that 'combinations of few characteristics often combine in populations to uniquely or nearly uniquely identify some individuals.'[34] As a consequence,

28 Michele Finck and Frank Pallas (2020) Op. cit., p. 15.

29 Gerald Spindler and Phillip Schmechel (2016), 'Personal Data and Encryption in the European General Data Protection Regulation' 7 JIPITEC 163.

30 Bjørn Aslak Juliussen, Elisavet Kozyri, Dag Johansen, Jon Petter Rui (2023) The third country problem under the GDPR: enhancing protection of data transfers with technology, International Data Privacy Law, Volume 13, Issue 3, August 2023, Pages 225–243, https://doi.org/10.1093/idpl/ipad013

31 Alexandre Lodie (2023). Are personal data always personal? Case T-557/20 SRB v. EDPS or when the qualification of data depends on who holds them. https://hal.science/hal-04292464/

32 Nadezhda Purtova (2018) 'The law of everything. Broad concept of personal data and future of EU data protection law' Law, Innovation and Technology, 10(1), 40-81. https://doi.org/10.1080/17579961.2018.1452176. See also Bart van der Sloot (2020). Regulating non-personal data in the age of Big Data. In Health Data Privacy under the GDPR (pp. 85-105). Routledge and Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques Adopted on 10 April 2014.

33 Sophie Stalla-Bourdillon and Alison Knight (2016) Anonymous data v. personal data-false debate: an EU perspective on anonymization, pseudonymization and personal data. Wis. Int'l LJ, 34, 284.

34 Latanya Sweeney (2000) Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2

some authors have argued that since technology moves forward, it might be simpler to just let go of the idea of personal data and govern just 'data' instead:[35] 'If processing metadata can be just as or even more revealing than processing content data; [...] then the question is whether the underlying rationale for the categorisations should be upheld.'[36]

According to Article 4(1) GDPR, 'personal data means any information relating to an identified or identifiable natural person.' Therefore, the 'identifiability' criteria will be crucial to determine whether a piece of data is personal or not, and whether the GDPR applies. However, the identifiability criteria are not clear from the text of the law. Actually, this has been one of the most studied questions by the GDPR scholarship since the regulation was adopted in 2016. According to Article 29 Data Protection Working Party, in general terms, a natural person can be considered as 'identified' when, within a group of persons, he or she is 'distinguished' from all other members of the group. Accordingly, the natural person is 'identifiable' when, although the person has not been identified yet, it is possible to do it […].[37] Further, identification is normally achieved through pieces of information which we may call 'identifiers' and which hold a particularly privileged and close relationship with the particular individual. Examples are outward signs of the appearance of this person, like height, hair colour, clothing, etc. According to the Working Party, it depends on the specifics of each case whether or not the data allow for the identification of an individual and whether or not the information can be regarded as anonymous. A case-by-case analysis should be conducted, paying special attention to the degree to which the means are likely and reasonably to be used for identification.[38]

Although the jurisprudence from the Court of Justice of the European Union (CJEU) has helped to clarify the terms of the definition of personal data and the 'identifiability' criteria (i.e. a broad interpretation of the notion of personal data),[39] the question is far from being solved. In this regard, the CJEU has considered that IP addresses combined with the additional information held by the Internet service provider necessary to identify the data subject and the written answers submitted by a candidate at a professional examination and the examiner's comments with respect to those answers were personal data (adopting an 'absolute approach').[40] On the other hand, very recently, the EU General Court considered that comments identifiable via an alphanumeric code and the re-identification of a person by journalists from information published in a press release were not personal data (i.e., following a 'relative approach').[41] The key element that might differentiate between the 'absolute' and the 'relative' approach to the notion of personal data is the means available for re-identification. According to the CJEU, if the data processor/controller has "the legal means which enable it to identify the data subject with additional data [...] about that person",[42] we will be moving within the realm of personal data. But the Court also argued that only legitimate methods of identification that do not actually involve an excessive amount of work should be taken into account.[43] In this vein, in *Single Resolution Board*,[44] the EU General Court claimed that regardless of whether the data might be regarded as "pseudonymized by nature," the EDPS should have evaluated whether, in this particular situation, the data receiver had measures reasonably likely to be carried out to re-identify the data.[45] Therefore, not just if such measures existed and they were available, but whether they were within the reach of the data recipient. According to the scholarship, this should be operationalized in light of the time and financial resources that the potential re-identifier will require to re-identify the data.[46]

Another question is that of the real value of processing non-personal data. According to Stal-

35 Bart van der Sloot (2017) Privacy as virtue. Cambridge: Intersentia.
36 Bart van der Sloot (2020) Regulating non-personal data in the age of Big Data. In Health Data Privacy under the GDPR 99 Routledge.
37 Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data Adopted on 20th June, 12
38 Ibid.
39 Bart van der Sloot (2020) Regulating non-personal data in the age of Big Data. In Health Data Privacy under the GDPR 99 Routledge.
40 See, for instance, C-582/14 Patrick Breyer v. Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779 and C-434/16, Peter Nowak v. Data Protection Commissioner ECLI:EU:C:2017:994.
41 Case T-557/20, Single Resolution Board v. EDPS [2023] ECLI:EU:T:2023:219. (It should be noted that this judgement has been appealed by the EDPS precisely on the ground that the General Court did 'not give consideration to the notion of pseudonymisation') and T-384/20 OC v Commission ECLI:EU:T:2022:273
42 C-582/14, Paragraph 49
43 Paragraph 46.
44 Case T-557/20, Single Resolution Board v. EDPS [2023] ECLI:EU:T:2023:219.
45 Case T-557/20, Paragraph 103
46 Alexandre Lodie (2023) Op. cit. See also Gerald Spindler and Philipp Schmechel (2016) Personal Data and Encryption in the European General Data Protection Regulation, 7 JIPITEC 163 para 1.

la-Bourdillon and others, finding patterns, or establishing connections between data points, maximises the value of information that may be obtained from dataset analysis (especially when utilising automatic algorithmic tools). However, anonymization seeks to break down these linkages between data points inasmuch as they pertain to information that may be discovered about particular individuals and their identities.[47] In Ohm's words, '[d]ata can be either useful or perfectly anonymous but never both.'[48] Legal uncertainty arises from this unclear regime and, as will be further discussed later in the paper, this might be a big concern for international data transfers. One may argue that because pseudonymised datasets are regarded as non-personal, at least in the hands of a data receiver who is unlikely to re-identify them, they can be sent to a third party (i.e. outside of the EU).

According to the literature,[49] three different perspectives on the definition of anonymous data under data protection legislation are emerging. The 'harm-based' approach, the 'risk-based' approach and the 'procedure-based' approach. The 'harm-based' approach specifically depends on the explicit identification of harm associated with inadequate anonymization. However, effective reidentification efforts can be exceedingly challenging to prove *a posteriori,* because they are frequently concealed. This approach also faces challenges since it relies on proving that the inadequate anonymization technique was the cause of legally identifiable harm. Second, under a 'risk-based approach', scholars argue that the definition of anonymous data in law should also be based upon a case-by-case assessment of the facts, but using an *ex-ante* evaluation of the potential risks of re-identification on the basis of any given data in the particular circumstances.[50] Such an approach implies that regular assessments of the risks associated with re-identification should be carried out, including when the data is reused. However, traditional risk-based approaches remain essentially output-based. According to Quelle, '[w]hile a pure risk management approach would focus only on the procedures taken to assess and mitigate risks, a pure harm-based approach attaches legal consequences only to the outcome that is achieved. Harm-based approaches are about abolishing "design" or "output" obligations in favour of a more ex post, outcome-oriented review.'[51] Finally, under a 'procedure-based' security approach, the legislation may be crafted around the processes required to reduce the danger of re-identification and the disclosure of sensitive attributes, rather than concentrating on the ultimate aim of anonymization. To put it in another way, the 'procedure-based' model, like other process-based regimes, requires processes rather than results. Although this model has some elements of the risk-based approach—for instance, it mandates conducting a risk assessment before sharing data— it remains focused on the idea of minimising risks. Therefore, procedure-based approaches also include a risk-tolerant approach to data release policies that builds upon statistical disclosure limitation techniques.[52]

On the risk-based group, a novel and interesting approach is the one proposed by Rupp and others,[53] who claim that data must only be considered personal where there is a clear (real) threat to a fundamental right. The purpose and result elements are effective analytical techniques for determining the presence of a given risk. While partially overlapping, these three factors can help identify which fundamental rights are directly harmed by data processing and why. Risks can arise from the data content, particularly if there is information protected by the Right to Privacy under Art. 7 Charter of Fundamental Rights of the European Union (hereinafter, the Charter). This applies regardless of the data controller's or third party's purpose or the impact on the data subject (about element). Risks can also arise from the specific purpose for which the data is being processed, either because it is directly related to a negative outcome (or impact) on any fundamental right or because the data

47 Sophie Stalla-Bourdillon, & Alison Knight (2016), Op. cit.

48 Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010, U of Colorado Law Legal Studies Research Paper No. 9-12, Available at SSRN: https://ssrn.com/abstract=1450006 (last access 4.9.2024)

49 Ira Rubinstein and Woodrow Hartzog, Anonymization and Risk (August 17, 2015). 91 Washington Law Review 703 (2016), NYU School of Law, Public Law Research Paper No. 15-36, Available at SSRN: https://ssrn.com/abstract=2646185

50 Ohm, Paul (2009) Op.cit.

51 Claudia Quelle, Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. European Journal of Risk Regulation. 2018;9(3):502-526. doi:10.1017/err.2018.47

52 Ira Rubinstein and Woodrow Hartzog (2016) Op.cit.

53 Valentin Rupp and Max von Grafenstein (2024) 'Clarifying "Personal Data" and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) through Refining the Concept of Data Protection' 52 Computer Law & Security Review 105932 <https://www.sciencedirect.com/science/article/pii/S0267364923001425> accessed 30 March 2024.

is being used to evaluate a person, posing a specific risk to the autonomy of the data subjects as protected by the Right to Data Protection under Art. 8 of the Charter (purpose element). Second, the potential negative outcome of data processing poses a distinct risk to any other basic right. To properly assess privacy risks, it is important to distinguish between three types of privacy impacted by data processing: core privacy, which includes intimate information and private conversations; the regular private sphere, which includes anything hidden from others; and privacy in public, which includes anything done in public. According to Rupp and others, personal data anonymisation is only significant in relation to the about element, as non-personal and hence anonymised data can always be linked to a person through a specific purpose or result (i.e. how the data is used). Therefore, anonymisation techniques are only adequate for information pertaining to the fundamentals of privacy once it is no longer possible to link the information to a specific individual, regardless of that person's real identity, including name or address. It is sufficient for information pertaining to the ordinary private sector that the individual is no longer recognisable in social situations. It is sufficient for information about the public domain that cannot be combined with other data to create personal profiles and learn more about an individual. These needs can be guaranteed according to the sector affected with respect to the purpose and result elements, by defining and monitoring controlled processing environments. Thus, organisational and technical actions can have an impact on the legal determination of whether data is considered personal or non-personal. They function as legal compliance measures to ensure that data protection law does not become relevant later, since it is not even applicable to begin with when we are dealing with non-personal data. On the other hand, van der Sloot argues that '[t]he material scope of the right to data protection is not dependent on the existence of individual harm but determined by the question of whether the data can be used to identify a person.'[54]

A final consideration concerns the technical feasibility of pseudonymisation. According to the scholarship,[55] pseudonymisation does not fulfil what it promises. There have been numerous cases where it was widely demonstrated that, initially pseudonymised databases allowed researchers (but also potentially not very skilled people) to re-anonymize the subjects present in them. Because of this, Ohm proposes a complete re-conceptualization of data protection legislation criteria including the trust of the subject's recipient of the information, the private or public character of the release of the information, the sensitivity of the data, the contextuality of the accessing operation,[56] and a stricter enforcement regime, among others. We propose another approach which is based on the practical importance of the protection of the data. Building somehow in the case-by-case perspective that was presented before, we think a more tailored approach based on the practicalities of the data processing operation would be a more tailored solution to the digital era. According to the latter approach, the protection of the data will not be necessarily based within its personal, non-personal or pseudonymised character, but on when, practically speaking, does it matter that such data are protected. For instance, it could matter because it is virtually possible to identify the data subject from the data or because a data breach could entail disastrous consequences from a privacy or financial point of view. On the other hand, it might not matter when the data is immediately deleted after collection or in open public registers.

In such a midst of uncertainty, several Regulations part of the EU data *acquis* tackle the question of data anonymisation, giving us a hint of its relevance. References to data anonymisation can be found within the GDPR but also the AI Act,[57] the DGA, the DMA and the DA.

4. Anonymisation under the EU Data *Acquis*

The EU data *acquis* is built upon 4 building blocks: personal data, non-personal data, anonymous data, and pseudonymous data. These four categories sometimes intertwine, such as pseudonymous

54 Bart van der Sloot (2020) Op. cit.

55 Ohm, Paul (2009) Op.cit.

56 Sebastian Benthall, Seda Gürses and Helen Nissenbaum (2017) Contextual integrity through the lens of computer science. Foundations and Trends® in Privacy and Security, 2(1), 1-69.

57 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). OJ L-2024/1689, 12.7.2024.

data, which become non-personal data due to an anonymization process. The current conceptualization of these categories is established in the GDPR. Later additions to the EU data *acquis*, such as the AI Act, the DMA, the DGA and the DA, which were passed after the GDPR, consider the above mentioned categories.

These regulations of the EU data *acquis* acknowledge the categories of pseudonymized and anonymized data, even though they do not define them. For instance, the AI Act refers to anonymization and pseudonymization in the context of data security requirements in compliance with personal data regulations when Artificial Intelligence systems process personal data. In principle, all personal data processed by AI systems should be either anonymised when possible or at least pseudonymized in cases such as in the processing of special categories of data for bias detection and correction in high-risk AI systems (Article 10(5)(b). Consequently, even when the AI Act does not have its own definition of what anonymous and pseudonymous data are, it is fair to assume that they have adopted the GDPR definitions, considering that such concepts appear within the context of compliance with the data protection regulations when personal data is processed by AI systems.

The Data Governance Act follows the same pattern. Regarding conditions for re-use, it states that the protected nature of data should be preserved 'in accordance with Union and national law', which could include anonymisation (and pseudonymisation) requirements, according to its Article 5(3). Same for the Digital Markets Act, which requires compliance with 'Union data protection and privacy rules and principles […] including by providing business users with duly anonymized data where appropriate.'[58] Finally, along the same lines, the Data Act establishes that when,

> "Strictly necessary to include personal data in the data made available to a public sector body or to a Union institution, agency or body the applicable rules on personal data protection should be complied with and the making available of the data and their subsequent use should and be accompanied by safeguards for the rights and interests of individuals concerned by those data. [...] The data holder should take reasonable efforts to anonymise the data or, where such anonymisation proves impossible, the data holder should apply technological means such as pseudonymisation and aggregation, prior to making the data available."59

To sum up, we could argue that the GDPR's notions of personal, non-personal, pseudonymised and anonymized data are also applicable in the context of the AI Act, the DGA, the DMA and the DA, since the latter legislations directly refer to the GDPR application in the context of the processing on personal data.

Nevertheless, the GDPR conceptualization does not necessarily reflect the positions expressed in the literature (discussed in the previous section) and the technical feasibility of anonymization techniques. With regard to technical feasibility, as discussed in the previous section, pseudonymization is very difficult to achieve in practice, due to the increase in computing power and the vast amount of data available nowadays. As far as the literature is concerned, as previously argued, the current discussion is more inclined to the deletion of the categories of personal, pseudonymised and non-personal data. The different approaches argue to discuss the processing of (personal) data on a case by case basis or to shift the focus to the trust of the subjects recipient of the information, the private or public character of the release of the information, the sensitivity of the data, the contextuality of the accessing operation, or the practical importance of the processing operation. Finally, the need for a clearer enforcement regime will be crucial, also when it comes to the international transfer of the data.

5. International Data Transfers

In the previous section, the paper discussed the complex framework stemming from the catego-

58 Supra, Art. 13(5) DMA.
59 Recital 64 Data Act.

rization of data in personal and non-personal and the role of pseudonymisation and anonymisation in such a context. The paper turns now to discuss international data transfers and the approaches taken by different pieces of EU legislation, particularly the GDPR, the DGA and the DA in relation to this topic.The focus on these three pieces of legislation is driven by two main reasons: first, because the GDPR establishes the EU's regulatory framework for data protection rights, including the rules governing international transfers of personal data outside the EU; second, because the DGA and the DA are recent EU regulations that, while addressing international transfers of non-personal data, provide a point of comparison in terms of the legal regimes they apply. This is especially relevant as they incorporate some concepts from the GDPR, which are explored further in this paper.

As discussed in the introduction, cross-border data transfers to countries outside of the European Economic Area (EEA) constitute an essential part of the global economy, allowing businesses and consumers to access the best available technology and services, wherever those resources may be located. This flow of data across borders benefits all industry sectors, from manufacturing to financial services, health care and beyond, in different ways, such as providing goods and services to customers, managing a global workforce, and maintaining supply chains. However, the regulatory changes in terms of data protection that have taken place since 2016 with the implementation of the GDPR, and more recently with the adoption of the DA and the DGA, pose challenges for countries outside the EU data space as they may impose trade barriers due to complex data compliance elements required by EU legislation.[60]

Although there are critiques raised in the literature on the topic over the current state of affairs relating to cross-border transfers of personal data to third countries, such as being disproportionate, ineffective, and unforeseeable,[61] the rules established under Chapter V of the GDPR are precise in formulating the tools that allow for the transfer of personal data outside the EEA area. Moreover, the European Data Protection Board (EDPB) and national regulatory authorities have been active in working on the interpretation and eventual gaps that need to be filled.[62] In our view, the key point of controversy in international data transfers lies in determining the applicable legal framework, which depends on whether the data is classified as personal or non-personal. This classification ultimately dictates the rules that will govern the transfer. If the data is deemed personal, the GDPR regime applies. On the other hand, if the data is considered non-personal, the rules governing the transfer are determined by the specific contractual agreements between the parties involved—namely, the data exporter and the data importer/recipient.. However, as further discussed in the coming pages, even international transfers of non-personal data are increasingly regulated under the DA and the DGA, adding more complexity to the applicable legal framework.

5.1. *Transfer of Personal Data under the GDPR*

The export of personal data from the EEA to third countries requires alignment with a series of criteria and conditions established by Chapter V of the GDPR. Although the GDPR does not provide for what constitutes an "international data transfer", the EDPB, with a view to clarify the interplay between the territorial application of the GDPR (Article 3) and the rules relating to international data transfers provided by Chapter V GDPR, has identified three cumulative criteria to define a data processing operation as an international data transfer: 1) the controller or processor ("exporter") is subject to the GDPR for the processing activity in question; 2) the "exporter" makes available or discloses personal data involved in the processing activity in question to another controller or processor ("importer"); the "importer" is located in a third country, irrespective of whether or not this importer is subject to the GDPR for the processing activity in question (Article 3) or is an international organi-

60 Fredrik Erixon, Philipp Lamprecht, Erik van der Marel, Elena Sisto, Renata Zilli (2024) The extraterritorial impact of EU Digital Regulations: how can the EU minimise adverse effects for the neighbourhood? Policy Paper, European Centre for International Political Economy (ECIPE), January 2024. DOI 10.1158672024006

61 Bjørn Aslak Juliussen, Elisavet Kozyri, Dag Johansen, Jon Petter Rui (2023) Op. cit, p. 230.

62 See, for instance, EDPB (2023) Guidelines 5/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. With regard to NRAs, see, for example, the Guidelines from the Spanish authority on Anonymisation available at https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf (last access 4.9.2024) and the Irish DPC Guidance on Anonymisation and Pseudonymisation available at https://www.dataprotection.ie/sites/default/files/uploads/2022-04/Anonymisation%20and%20Pseudonymisation%20-%20latest%20April%202022.pdf (last access 4.9.2024)

sation.[63]

In addition, the transfer of personal data to a non-EEA country or international organisation requires the compliance with the GDPR's basic processing principles: having an appropriate legal basis for processing; ensuring that the necessary security measures are implemented and that the controller only processes the personal data necessary for the specific processing activity (i.e., principle of data minimisation).

According to the GDPR there are three main ways to transfer data outside the EEA area. The first one concerns transfers on the basis of an adequacy decision adopted by the European Commission (i.e., Article 45 GDPR). In this case, the third country or the international organisation in question must have an "equivalent level of data protection" to that existing in the EEA area according to an assessment by the European Commission.[64] The second way refers to transfers subject to 'appropriate safeguards' (i.e., Article 46 GDPR). The appropriate safeguards that may be used to transfer personal data to non-EEA countries in the absence of adequacy decisions can be provided by the different transfer tools listed in Article 46(2) GDPR, namely: standard contractual clauses (SCCs); binding corporate rules (BCRs); codes of conduct; certification mechanisms; and *ad hoc* contractual clauses.

Among the appropriate safeguards listed in Article 46, SCCs stand as the most relevant. First because they are "off the shelf" and easy to implement, since SCCs are pre-approved by the EC. Therefore, they offer a model that allows data controllers, processors (importers or exporters) to comply with the EU rules, being particularly beneficial to small businesses that often do not have the resources to negotiate individual contracts with each of their trading partners.[65] SCCs can be in fact incorporated in the commercial contractual frameworks of the activities involving international data transfers, though parties are not obliged to use the SCCs pre-approved by the EC. Secondly, SCCs are indeed the most widely used international data transfer tool for EU companies; according to surveys from IAPP and DIGITALEUROPE, around 85% of the EU surveyed companies use SCCs.[66]

Since the entry into force of the GDPR, the EC has adopted two sets of SCCs: one set of clauses for the relationship between controllers and processors, and another set as a tool to be used for data transfers.[67] This second set was adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021. These new sets of SCCs were adopted after the remarkable case Schrems II.[68] In this decision - ruled almost five years after Schrems I[69] - the CJEU not only declared invalid the EU-U.S. Privacy Shield framework,[70] i.e., the adequacy decision for transatlantic exchanges of personal data for commercial purposes after the Safe Harbour invalidation,[71] but also stipulated stricter requirements for the transfer of personal data based on SCCs.

Accordingly, in *Schrems II* the CJEU reminded that SCCs and the other transfer tools mentioned

63 EDPB (2023) Op. cit, p. 7.

64 So far the EC has adopted adequacy decisions for: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom, United States (commercial organisations participating in the EU-US Data Privacy Framework), and Uruguay. See https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en (last access 4.9.2024)

65 European Commission. Frequently asked questions on the new SCCs EC. See https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en (last access 4.9.2024)

66 See https://f.hubspotusercontent20.net/hubfs/525875/IAPP_EY_Governance_Report_2019.pdfn (last access 4.9.2024) See also https://www.digitaleurope.org/news/schrems-2-data-transfers-survey-85-of-companies-in-europe-use-standard-contractual-clauses/ (last access 4.9.2024)

67 See https://commission.europa.eu/document/download/e60b1cd4-d802-44d5-9cac-ddd3c943a5ef_en?filename=1_en_annexe_acte_autonome_cp_part1_v5_0.pdf (last access 4.9.2024)

68 Case C-311/18, Schrems II [2020] ECLI:EU:C:2020:559.

69 Case C-362/14, Schrems I [2015] ECLI:EU:C:2015:650. The case stems from a complaint issued by Maximilian Schrems against the Irish Data Protection authority. This complaint challenged the validity of the use of Safe Harbour agreement - the adequacy decision for EU-US commercial data transfers adopted under Directive 95/46/EC - by Facebook, due to concerns about the access of personal data by the US government for surveillance purposes. Since the Irish authority declined to investigate the complaint, the plaintiff appealed the decision before the Irish Court, which then referred the case to the CJEU for a preliminary ruling. Among other findings, the Court declared the Safe Harbour agreement invalid.

70 The Privacy Shield was adopted by the EC in July, 2016. See https://ec.europa.eu/commission/presscorner/detail/it/memo_16_2462

71 See https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520 (last access 4.9.2024)

in Article 46 GDPR do not operate in a vacuum. Therefore, controllers or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. In the landmark ruling, the Court left open the possibility for exporters to implement supplementary measures that fill the gaps in the protection and bring it up to the level required by EU law. Although the CJEU does not specify which measures could be adopted, it underlined that exporters would need to identify them on a case-by-case basis. Following the *Schrems II* ruling, the EDPB adopted Recommendation 01/2020.[72] This document indicates in six stages a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place by data exporters to third countries to ensure an equivalent degree of protection to the EU. In short, the six steps advise data exports the following: 1) to map all the data transfers to third countries, verifying that the data transferred is adequate, relevant and limited to what is necessary; 2) to verify the adequate transfer tool to rely on - adequacy decision; appropriate safeguards or derogations; 3) to carry out a due diligence exercise and a documented assessment of the legal framework for data protection in the third country; 4) to adopt technical (e.g., pseudonymisation, encryption), contractual (e.g., contractual arrangements containing additional obligations on transparency or on the use of specific technical cyber-security measures) and organisational (e.g., adoption of internal privacy with with clear allocation of responsibilities for data transfers, adoption of internal accountability procedures); 5) to verify the adequate formal procedures to be followed depending on the transfer tool used, consulting the competent supervisory authority; and 6) to periodically reassess the level of protection of personal data transferred to third countries and monitor any changes that may affect it.

Schrems II has provoked criticism in the academic literature when it comes to the level of protection of personal data required from third countries. For some, by concluding that "appropriate guarantees" means that all international transfers to third countries should ensure "a level of protection essentially equivalent to that which is guaranteed within the European Union", the CJEU establishes that there is only one standard of protection, equating the notions of appropriate safeguards, adequate level of protection, and equivalent level of protection, irrespective of the wording of Article 44 GDPR, and thus creating legal uncertainty.[73] Therefore, the standard required by the CJEU in *Schrems II* for the transfer of personal data to third countries is so high that it may prove difficult to meet.[74] In the same lines, it has been argued that the findings on *Schrems II* together with Recommendation 01/2020 have changed the provisions of the GDPR, raising the bar for international personal data transfers, using other transfer mechanisms than adequacy decisions,[75] and making it extremely difficult for small businesses to comply with such requirements.[76]

The last mechanism for the transfer of personal data to third countries provided by the GDPR are 'derogations' for specific situations. Derogations are considered of an exceptional nature and are thus used in the absence of an adequacy decision or of appropriate safeguards. According to Article 49 GDPR, derogations can be used when: the data subject provides an explicit consent; they are necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request; necessary for the performance of a contract made in the interests of the individual between the data controller and another person; necessary for important reasons of public interest; necessary for the establishment, exercise or defence of legal claims; necessary to protect the vital interests of the individual in question or other persons, where the individual is physically or legally incapable of giving consent; or made from a register which under the national law of an EEA country or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate

72 EBPD (2020) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, p. 3.

73 Case C-311/18, Schrems II, para. 96.

74 Zuzanna Gulczyńska (2021) A certain standard of protection for international transfers of personal data under the GDPR, International Data Privacy Law, Volume 11, Issue 4, November 2021, Pages 360–374, https://doi.org/10.1093/idpl/ipab013

75 Paul Breitbarth (2021) A Risk-Based Approach to International Data Transfers European Data Protection Law Review Volume 7, Issue 4, pp. 539 - 549. DOI: https://doi.org/10.21552/edpl/2021/4/9

76 Corrales Compagnucci, Marcelo and Aboy, Mateo and Minssen, Timo, Cross-Border (2021) Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses. Vol. 4 No. 2: Nordic Journal of European Law Issue 2021(2). https://doi.org/10.36969/njel.v4i2.23780

interest in inspecting the register).Furthermore, a necessity test must be conducted to evaluate whether the transfer is essential and, consequently, to determine if it serves the specific purpose of the applicable derogation..[77]

As shown in this Section, the interpretation of the GDPR rules on international transfers of personal data has become increasingly tightened after the *Schrems II* ruling. For instance, for the transfer to take place on the basis of appropriate safeguards, such as Standard Contractual Clauses (SCCs) mechanism, the data exporter needs to assess whether the third country has an essentially equivalent level of protection of personal data as the one granted in the EU. As commentators have argued, setting a very strict standard of protection for the transfer of personal data to third countries could have a deterrent effect in the context of the digital economy. Many countries, in fact, do not provide the same level of protection as the EU and, as a consequence, some European companies would not be able to export personal data to countries outside the EEA.[78] In view of these considerations, complying with the rules on the transfer of personal data to third countries may not be trivial to many EU data exporters.

This complexity should not affect the transfer of non-personal data; since this type of data export to third countries is not subject to the GDPR rules, the CJEU case-law and the EDPB recommendations are not applicable. In accordance with the arguments put forward in the previous sections of this paper, international transfers of non-personal data could be subject to changes in the applicable legal framework in the case data becomes re-identifiable, making the discussion on the distinction between personal and non-personal data relevant also in the realm of international data transfers. Moreover, this situation tends to become increasingly complex considering the set of new EU digital Regulations which call into question the 'personal/non-personal' data dichotomy, especially the DAt and the DGA, which will be analysed in the following sub-section.

5.2. International Data Transfer under the Data Act (DA) and the Data Governance Act (DGA)

The DA and the DGA aim at facilitating access to data in a reliable and secure manner. While the DGA establishes a framework to boost data sharing, regulating the data reuse, the DA establishes rules for the access and use of data generated by private actors in the European digital economy. The DA will apply from 12th September 2025, whereas the DGA is applicable from September 2023.

These two pieces of EU law also lay down rules on international data transfers. However, such rules apply only to transfers of non-personal data, as transfers of personal data continue to be regulated by the GDPR, as explained in the previous section. In this regard, both the DGA and the DA provide for restrictions on international transfers or access to non-personal data generated in the EU. The aim of these restrictions is to prevent 'protected' non-personal data generated in the EU from being transferred to third countries without sufficient protection of intellectual property rights, trade secrets, confidentiality, and other EU interests. As we will demonstrate in the following sections, these new EU regulations may add additional complexity to international data flows.

5.2.1. Data Act (DA)

The DA provides for rules for the fair access to and use of data, establishing contractual obligations on international access and transfer of non-personal data, and thus creating a kind of new layer of protection for these international data access requests and transfers.[79] According to Article 32 of the DA, providers of data processing services shall take technical, legal, and organisational measures to prevent non-personal data transfers in breach of EU law or Member States law. In this line, and applying the same logic of the GDPR, under the DA cross-border data flows with third countries are subject to the protection afforded to data transfers within the EU. Article 32(2) DA provides that this protection can be ensured by international agreements between the EU and a third country, or between a Member State and a third country. However, in the absence of these agreements, the

77 See https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en (last access 4.9.2024)

78 Thomas Espeel, Eléonore Colson, Alexandre Cruquenaire (2022) International data transfers under GDPR: applicable requirements and practical implementation. Le droit des affaires, (141), 19-41.

79 Bárbara da Rosa Lazarotto and Gianclaudio Malgieri (2023) The Data Act: a (slippery) third way beyond personal/non-personal data dualism? European Law Blog: News and Comments on EU law https://europeanlawblog.eu/2023/05/04/the-data-act-a-slippery-third-way-beyond-personal-non-personal-data-dualism/ (last access 4.9.2024)

transfer of data can only take place if the requirements listed in Article 32(3) are met, namely:

a) the third-country system requires the reasons and proportionality of such a decision or judgment to be set out and requires such a decision or judgment to be specific in character, for instance by establishing a sufficient link to certain suspected persons or infringements.

b) the reasoned objection of the addressee is subject to a review by a competent third-country court or tribunal; and

c) the competent third-country court or tribunal issuing the decision or judgment or reviewing the decision of an administrative authority is empowered under the law of that third country to take duly into account the relevant legal interests of the provider of the data protected by Union law or by the national law of the relevant Member State.

In addition, providers of data processing services responsible for the transfer of data to third countries should also adopt - and publish on their websites - technical measures, such as encryption, audits and compliance with certification schemes, to prevent access to the systems where they store non-personal data. In addition, where possible, they should inform their customers about the measures adopted before granting access to their data. In other words, the data processor should guarantee the safety of its database vis-à-vis cyberattacks and it should inform its customers of the measures adopted to this regard. Recognising that this requirement could be burdensome for data service providers, the European Commission, together with the European Data Innovation Board (EDIB) and a group of experts, will assist in assessing whether the conditions set out in Article 32(3) DA are met.[80]

5.2.2. Data Governance Act (DGA)

The DGA is a cross-sectoral legal instrument aiming at regulating the re-use of publicly stored, protected data, providing rules for international transfers by the re-user of certain constellations of non-personal and personal data. Despite the application of the GDPR rules to the transfer of personal data, the DGA establishes, in addition, inbuilt safeguards to increase trust in data sharing and reuse, a prerequisite for making more data available on the market.

With regard to the international transfer of non-personal data, though the GDPR rules do not apply, the DGA establishes similar safeguards for access requests from third country governments.[81] Indeed, the contractual obligations for the transfer of non-personal data under Article 5(9) DGA are guided by the accountability mechanism described in Recital 59. The latter provision recalls the standard contractual clauses of Article 46 GDPR. Moreover, the DGA establishes in its Article 5(12) a type of adequacy assessment to evaluate the level of protection of intellectual property and trade secrets protection in the third country receiving non personal data. As discussed above, the adequacy regime has its drawbacks, especially in terms of complaints before the EU Courts, as *Schrems I* and *Schrems II* well demonstrate.[82] For instance, it took three years to the adoption of a new adequacy decision between the EU and US after the invalidation of the Privacy Shield in Schrems II.[83]

Similarly to the DA, the DGA seems to embrace a blurred boundary between personal and non-personal data, by creating a kind of hybrid category of 'highly sensitive' non-personal data.[84] The transfer of this data to third countries will be limited when it "may lead to the risk of re-identification of non-personal, anonymised data."[85] Consequently, according to Article 5(13) DGA, the distinction between personal and non-personal data is not clear-cut, showing that the irreversible nature of

80 European Commission. The Data Acta explained: A comprehensive overview of the Data Act, including its objectives and how it works in practice. https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained (last access 4.9.2024)

81 European Commission. Data Governance Act explained. https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained (last access 4.9.2024)

82 Yuliya Miadzvetskaya (2023) Data Governance Act: On International Transfers of Non-Personal Data and GDPit Mimesis. European Data Protection Law Review (1) 2023, p. 13.

83 Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (notified under document C(2023)4745).

84 See, for instance, Recital 24 and Art. 5(13) DGA.

85 Ibid.

anonymisation may be questioned and that some data initially considered non-personal can, in fact, be re-identified, consequently regaining their status as personal data.[86]

To sum up, while the EU Data Strategy[87] recognises the importance of an open approach to international data flows and the potential that international data transfers with the vast amount of data generated in the EU could enhance the Union's competitiveness in the global arena, the extension of the GDPR logic and standards to the transfer of non-personal data may trigger undesirable effects and slow down the EU's potential as a data exporter.

6. Conclusions

Data has become an essential input in the digital economy; having access to a large, updated and verified source of data is a key competitive advantage, allowing a firm to personalize its services for its customers and engaging in targeted advertising. In addition, data access is increasingly important to train AI models. At the same time, data easily 'moves' across the borders: Internet users may provide their data to a digital services provider based in another country; multinational corporations manage data centres established in different countries of the world; economic operators increasingly trade datasets in the contest of B2B data sharing.

During the past years, the EU has developed a complex regulatory framework (i.e. so-called EU data *acquis*), which essentially pursues two distinct goals: on the one hand, it aims at fostering B2B data sharing, to enhance the competitiveness of the EU digital economy. On the other hand, via the adoption of the GDPR in 2016, the EU has also opted for a high level of protection for personal data. Besides the GDPR, the EU digital *acquis* includes several legislations, such as the DA, the DGA, the DMA, as well as sector specific Regulations. These legislations overlap with each other, generating a complex 'legal puzzle', which is far from being complete and which may cause legal uncertainty for economic operators. Tensions between the goal of fostering data sharing and safeguarding data protection are particularly evident in the context of personal data. While non-personal data can be (almost) freely shared between economic operators based on contractual arrangements, data that identifies an individual may be shared only subject to the individual consent or in accordance with one of the GDPR legal bases for data processing. In such a context, the use of anonymization techniques should in theory reconcile these two diverging goals: if full-anonymisation is reached, the data shall not be considered 'personal' and thus would be subject to the non-personal data regulatory regime, rather than to the GDPR stringent requirements.

The paper aimed at 'reconstructing' the 'puzzle' of the EU data *acquis*, looking specifically at the case of international data transfers. As a preliminary step, the paper analysed the distinction between personal and non-personal data, as well as the pseudonymization and anonymization concepts, in light of the relevant literature, as well as CJEU case law and EDPB and Working Party 29 guidelines. Secondly, the paper has analysed the EU legislations applicable in the context of international data transfers, namely the GDPR, the DA and the DGA, as well as the relevant CJEU case law.

A number of authors and the EDPB argue that data should be considered anonymized only when it becomes *de facto* impossible to re-identify the data subject (i.e. absolute approach to data anonymization), while other authors have argued in favour of a 'relative' approach to anonymization. According to the latter approach, data anonymized by the controller becomes non-personal, and thus outside the scope of the GDPR application, unless there are 'realistic' chances that the controller may re-identify an individual via data combination. In other words, while the 'absolute' approach opts for a zero-risk to re-identification, the 'relative' approach considers only concrete/proved risks of identification, rather than highly theoretical ones. While Recital 26 GDPR seems to support the relative approach, the CJEU has been rather inconsistent in its case law on the required standard of anonymization, opting either for an 'absolute' or a 'relative' threshold of anonymization on a case-by-case basis. Since the other legislations part of the EU data *acquis* refer to the GDPR concepts of anonymization and pseudonymization, the anonymization standard indeed remains unclear, gen-

86 Alexandre Lodie (2023) Op. cit.

87 (European Commission (2020) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: a European Strategy for Data (COM/2020/66 final).

erating legal uncertainty for economic operators. In the context of the digital economy, following the absolute approach implies that anonymization is *de facto* impossible, since potentially the controller could always re-identify the data subject via data combination. Such an approach thus blurs the distinction between personal and non-personal data, thus substantially broadening the GDPR scope of application and potentially limiting the scope of B2B data sharing in contrast with the objectives of the EU Data Strategy.

The expansion of the GDPR requirements is also visible in the context of international data transfers. The GDPR has introduced a complex system of safeguards *vis-à-vis* the export of personal data from the EU to third countries. Such a transfer can take place only if the recipient country provides an 'adequate' level of data protection, which is comparable to the GDPR, or if the controller implements a number of 'appropriate safeguards', such as standard data protection clauses, binding corporate rules, codes of conduct, certification mechanisms, or ad hoc contractual clauses which implement the GDPR requirements. In *Schrems II*, the CJEU narrowed down the scope of 'appropriate measures', by requiring the controller that relied on SCC to verify whether the system of legal redress in the third country is sufficient to ensure an effective enforcement of the standard contractual clauses in accordance with the GDPR requirements. This interpretation implies a higher and uncertain standard of proof for economic operators, which is difficult to be met in practice.

Finally, it is also worth mentioning that the recently adopted DA and the DGA have also substantially expanded the system of protection in relation to transfers of non-personal data outside the EU. Article 5(9) DGA recalls the standard contractual clauses of Article 46 GDPR. Moreover, the DGA establishes in its Article 5(12) a type of adequacy assessment to evaluate the level of intellectual property and trade secrets protection in the third country receiving non personal data which resembles the GDPR adequacy decisions. One could ask what the implications of DA and DGA provisions to international data transfers of non-personal data are: should the GDPR safeguards for personal data transfers be also considered in this case, or data controllers should be free to set lower contractual standards for non-personal data? Considering the blurring distinction between personal v. non-personal data discussed in the paper, and since most of the international transfers involve a mix of personal and non-personal data, the GDPR safeguards are increasingly relevant in every type of international data transfer. In other words, there are few concrete cases of international data transfers that involves exclusively non-personal data (e.g. weather conditions). Secondly, the question is whether and to what extent the *Schrems II* case law would be applicable in the context of the DA and DGA. This is an open question: on the one hand, the DA and DGA draw inspiration from the GDPR in relation to mechanisms to authorize international data transfers of non-personal data. On the other hand, the protected interests to justify such mechanisms are clearly different: individuals' privacy v. IP rights and security considerations. It is worth bearing in mind that the DA will apply from 12th September 2025, whereas the DGA is applicable from September 2023. Therefore, it will be for the European Commission, regulatory authorities, as well as national and EU courts to balance these interests and to reply to this question in the coming years.

The EU data *acquis* pursues two goals: fostering B2B data sharing, while providing a high level of protection of personal data. International data transfers represent a good case study, which show how these goals may sometimes conflict, and how the EU tends to give preference to privacy protection over efficiency considerations linked to B2B data sharing. The paper has shown that the blurring distinction between personal and non-personal data, the narrow interpretation of anonymization techniques, the expansion of the 'appropriate measures' requirements in the GDPR, and the introduction of new rules for the transfer of non-personal data have a cumulative effect, which limits the ability of economic operators to engage in data processing activities outside the EU.

The EU data *acquis* is a complex legal puzzle, this paper has analysed only a part of the potential overlaps and inconsistencies within this complex legal framework. Further research is ahead of us; time will tell us if the puzzle may be fully reconstructed.

Authors

Natalia Menéndez González

European University Institute

natalia.menendez@eui.eu

Danielle Borges

European University Institute

Danielle.Borges@eui.eu

Marco Botta

European University Institute

marco.botta@eui.eu