Protecting EU Data Outside EU Borders under the GDPR

Kuner, Christopher Barth

Published in:
Common Market Law Review

DOI:
10.54648/cola2023004

Publication date:
2023

Document version
Publisher's PDF, also known as Version of record

Document license:
Unspecified

Citation for published version (APA):
Kuner, C. B. (2023). Protecting EU Data Outside EU Borders under the GDPR. *Common Market Law Review*, *60*(1), 77-106. https://doi.org/10.54648/cola2023004

Common Market Law Review **60**: 77–106, 2023.

PROTECTING EU DATA OUTSIDE EU BORDERS UNDER THE GDPR

CHRISTOPHER KUNER*

Abstract

The EU General Data Protection Regulation (GDPR) aims to protect personal data outside EU borders by its rules on territorial scope and its restrictions on international data transfers. Despite its importance in EU fundamental rights law, the purpose and interaction of the GDPR's protections of cross-border data processing have long been shrouded in confusion. Initiatives of EU bodies to interpret the GDPR's safeguards illustrate the need for EU law to demonstrate clarity and consistency in defending fundamental rights outside EU borders. Only by maintaining the high level of protection required by the GDPR and the Court of Justice, can the EU's ambitions of cross-border data protection be realized and the GDPR's influence in third countries be maintained.

1. Introduction

In recent years, concerns have grown about threats to the rights of EU individuals when their data is processed by parties in non-EU or EEA member states[1] or transferred to them. Prominent examples include widespread data misuse by Internet companies based outside the EU;[2] the so-called "Snowden revelations", which concerned electronic surveillance by US intelligence

* Professor of Law, Vrije Universiteit Brussel (VUB) and Co-Director, Brussels Privacy Hub; Associate, Centre of European Legal Studies, University of Cambridge; Visiting Professor of Law, Maastricht European Centre on Privacy and Cybersecurity, Maastricht University; Affiliate Professor, University of Copenhagen. The author is grateful for the valuable comments of Christopher Docksey, Laura Drechsler, Herke Kranenborg, Dan Svantesson, Gabriela Zanfir-Fortuna, and the editors and reviewers.

1. Throughout this article, the term "EU" will refer to both the European Union and the European Economic Area (EEA), in which the GDPR also applies.

2. See e.g. Esteve, "The business of personal data: Google, Facebook, and privacy issues in the EU and the USA", 7 *International Data Privacy Law* (2017), 36–47; European Data Protection Supervisor, "Opinion 3/2018, EDPS Opinion on online manipulation and personal data" (19 March 2018).

agencies;[3] and orders by third country governmental or law enforcement authorities to transfer data stored in the EU to them.[4]

EU law protects against threats to personal data originating from outside EU borders through data protection legislation, its interpretation by the Court of Justice of the EU, and its implementation by such entities as the European Commission and the European Data Protection Board (EDPB). The framework legislation for data protection in the EU is the General Data Protection Regulation (GDPR),[5] which covers data processing in both the public and private sectors. The successor to the former Data Protection Directive 95/46[6] (DPD), the GDPR is based on the standards of the EU Charter of Fundamental Rights[7] (the Charter). Aside from the ECJ, some other important bodies at EU level responsible for interpreting the GDPR include the EDPB and the European Commission. The EDPB was established under Article 68 of the GDPR as an independent body with legal personality and is composed of Member State data protection authorities (DPAs)[8] and the European Data Protection Supervisor (EDPS); it adopts common positions and guidelines, coordinates enforcement by the Member State DPAs, and takes other actions to implement the requirements of the GDPR. The Commission issues decisions on the adequacy of third countries' data protection standards, approves appropriate safeguards for data transfers, and conducts international negotiations on data protection issues on behalf of the EU.

The GDPR seeks to protect personal data against external threats through rules concerning the territorial scope of data protection law (contained in Art. 3), which includes its application to data processing by parties established outside EU borders in certain circumstances, and through restrictions on transfers of personal data outside the EU (contained in Chapter V, Arts.

3. See Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (MacMillan, 2014).

4. E.g. under the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act), HR 1625, Division V, 115th Congress, 23 March 2018. See Christakis and Terpan, "EU-US negotiations on law enforcement access to data: Divergences, challenges and EU law procedures and options", 11 *International Data Privacy Law* (2021), 81–106.

5. 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), O.J. 2016, L 119/1.

6. Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. 1995, L 281/31 (no longer in force).

7. Charter of Fundamental Rights of the European Union, O.J, 2010, C 83/2.

8. DPAs are independent authorities set up under Chapter VI GDPR and are charged with enforcing data protection law, among other tasks. For a detailed examination of their role and functions, see Hijmans, *The European Union as Guardian of Internet Privacy* (Springer, 2016).

44–50). Territorial scope rules are *inward-looking* in the object of their protection in that they are designed to protect individuals in the EU from actions taken by actors outside EU borders, and are *reactive* in that they apply when non-EU parties take certain actions with regard to the data of EU individuals. By contrast, data transfer rules are *outward-looking* in that they require personal data transferred to a third country to receive protections based on EU law, and are *proactive* in the sense of addressing risks to the data before they are transferred, i.e. they require the parties to the transfer to ensure that the data will receive protection before the transfer is initiated.[9]

The EU also enhances the protection of personal data outside its borders by promoting the GDPR as a model to be adopted by third countries,[10] which makes it more likely that EU data will be processed abroad under EU standards. This is accomplished through a variety of mechanisms, such as encouraging third countries to emulate EU law; engaging in international negotiations with them; and making access to benefits conditional on compliance with EU law.[11] The global influence of the GDPR is illustrated by the Executive Order on signals intelligence issued by US President Biden in October 2022,[12] which addresses "concerns that the Court of Justice of the European Union raised in striking down the prior EU-US Privacy Shield framework as a valid data transfer mechanism under EU law".[13]

The GDPR has been hailed as one of the EU's "greatest achievements in recent years",[14] and its importance is demonstrated by the ubiquity and economic and social importance of data processing. The ease by which data can be processed across national borders means that issues involving the

9. Art. 44 GDPR, stating that data may be transferred only if the conditions laid down in Chapter V are complied with, implying that such compliance must be ensured before the transfer ensues.

10. See regarding the global influence of EU data protection law, Bradford, *The Brussels Effect* (OUP, 2020), Kindle edition, pp. 131–156; Kuner, "The Internet and the global reach of EU law" in Cremona and Scott (Eds.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (OUP, 2019), pp. 112–145.

11. See Scott, "The global reach of EU law" in Cremona and Scott, ibid., pp. 21–63; Kuner, ibid., at 130–134.

12. US President Joseph R. Biden, "Executive Order on enhancing safeguards for United States signals intelligence activities" (7 Oct. 2022), available at <www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/> (all websites last visited 16 Nov. 2022).

13. The White House, "FACT SHEET: President Biden signs Executive Order to implement the European Union-U.S. Data Privacy Framework" (7 Oct. 2022), available at <www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/>.

14. European Data Protection Supervisor, "The history of the General Data Protection Regulation", available at <edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en>.

protection of EU fundamental rights against external threats often arise under the GDPR,[15] making data protection law a laboratory for the cross-border protection of rights. The GDPR also provides the baseline for the data protection standards contained in other EU legislation.[16]

The significance of the GDPR in EU law makes it important that there be consistent interpretation and implementation of its rules on cross-border data protection. Inconsistency in applying them may create gaps in protection; burdens for data controllers through the imposition of conflicting and duplicative obligations; and a lack of trust by individuals. The importance of clarifying the consequences of their interaction can be seen in the increased emphasis the Commission has put on initiatives to facilitate transborder data flows from the Union,[17] as illustrated by the adequacy decision covering data transfers to the US that it has said it will prepare following President Biden's announcement referred to above.[18] However, for many years little attention was paid to the relationship between territorial scope and data transfer rules and their respective roles, except by a few legal scholars.[19]

15. See e.g. Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP, 2017); Kuner, "Extraterritoriality and regulation of international data transfers in EU data protection law", 5 *International Data Privacy Law* (2015), 235–245; Ryngaert and Taylor, "The GDPR as *global* data protection regulation?", 114 *AJIL Unbound* (2020), 5–9, at 7–8, available at <www.cambridge.org/core/journals/american-journal-of-international-law/article/gdpr-as-global-data-protection-regulation/CB416FF11457C21B02C0D1DA7BE8E688>.

16. See e.g. 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), O.J. 2022, L 152/1, Recital 4, stating that it should be "without prejudice to Regulation (EU) 2016/679"; COM(2021)206 final, European Commission Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, p. 4, stating that the proposed AI Act is "without prejudice and complements the General Data Protection Regulation"; COM(2022)68 final, European Commission Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on the fair access to and use of data (Data Act), Recital 7, stating "This Regulation complements and is without prejudice to Union law on data protection and privacy, in particular Regulation (EU) 2016/679 …".

17. See COM(2017)7 final, "Communication from the Commission to the European Parliament and the Council, Exchanging and Protection Personal Data in a Globalised World", p. 8, stating that there are "new opportunities, notably through adequacy findings, to further facilitate data flows while guaranteeing the continued high level of protection of personal data"

18. See European Commission, "Questions & Answers: EU-U.S. Data Privacy Framework" (7 Oct. 2022), available at <ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045>, stating that "the European Commission will now prepare a draft adequacy decision"

19. See Granmar, "A reality check on the Schrems saga", 2 Nordic JIL (2021), 48–65; Hon, *Data Localization Laws and Policy* (Edward Elgar, 2017); Hon and Millard, "Data export in cloud computing – How can personal data be transferred outside the EEA? The cloud of unknowing, Part 4", Queen Mary School of Law Legal Studies Research Paper No. 85/2011, available at <papers.ssrn.com/sol3/papers.cfm?abstract_id=2034286>; Kuner, *European Data*

This article will first explain the legal requirements for cross-border data protection set out in the GDPR and their interpretation by the ECJ, and will then examine how they have been implemented by the EDPB and the Commission. It will show that that EU bodies have failed to adopt a consistent view of the principles underlying the cross-border protection of personal data, such as accountability, ensuring a high standard of protection, and the effective enforcement of fundamental rights. These failings can both impact the level of protection under EU law and undermine the GDPR's global influence. Finally, it will be argued that each of the relevant EU bodies (in particular the ECJ, the EDPB, the Commission, and the EU legislature) has a role to play in interpreting these rules in a way that realizes the GDPR's vision of cross-border data protection.

2. Legal requirements for cross-border data protection

2.1. *Introduction*

In order to understand how the GDPR protects against external threats to personal data, it is necessary to explain its rules on territorial scope and international data transfers. Their relationship in the text and structure of the GDPR will then be examined, before explaining the requirements for protection set out by the ECJ. Finally, the issues and questions that their interaction raises will be explored.

2.2. *Territorial scope rules*

The territorial scope of the GDPR is covered in Article 3 entitled "Territorial scope", the relevant provisions of which read as follows:[20]

> "1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

Privacy Law and Online Business (OUP, 2003), pp. 119–121; Kuner, *Transborder Data Flows and Data Privacy Law* (OUP, 2013), pp. 125–129; Kuner, "Territorial scope and data transfer rules in the GDPR: Realising the EU's ambition of borderless data protection", University of Cambridge Faculty of Law Research Paper No. 20/2021, available at <papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850>.

20. The quoted text omits Art. 3(3) dealing with application of the GDPR based on Member State law applying by virtue of public international law, which falls outside the scope of this article. See Jervis, "The curious case of Article 3(3) of the GDPR and its application to diplomatic missions", 10 *International Data Privacy Law* (2020), 107–114.

> 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

Application of the GDPR under Article 3(1) is based on personal data being processed in the context of the activities of an establishment of a data controller or data processor in the Union, so that it applies whether or not the data processing takes place in the Union and the individual is in the EU when their data is processed.[21] For example, in its *Google Spain* judgment, the ECJ applied Article 4(1)(a) DPD (which was equivalent to Art. 3(1) GDPR), covering data processing in the context of the activities of an establishment of a data controller in a Member State, to Google's search engine, even though the entity that was both the actual operator[22] and the data controller[23] of the engine was located in a third country.[24] The Court thus held that the processing of personal data by a search engine operated by an undertaking established outside the EU but with an establishment in an EU Member State was carried out "in the context of the activities" of such establishment and was thus subject to EU data protection law.

Concern that the DPD did not provide sufficient protection for personal data processed or transferred outside the EU led to the strengthening of territorial scope rules applicable to data processing by parties established outside the EU.[25] The GDPR applies to data controllers or processors not established in the Union when the conditions of Article 3(2) are satisfied; the mere accessibility of a website in the Union is not in itself sufficient.[26] Article

21. See EDPB, "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Version 2.1", at 10.

22. Case C-131/12, *Google Spain SL, Google Inc* v. *Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, EU:C:2014:317 (Grand Chamber), at para 43, second bullet.

23. Ibid., at para 60.

24. See Gömann, "The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement", 54 CML Rev. (2017), 567–590, at 571–572.

25. See COM(2012)9/3, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World—A European Data Protection Framework for the 21st Century", at pp. 10–11.

26. See Recital 23 GDPR.

3(2)(a) applies the GDPR to data processing by data controllers or data processors[27] not established in the EU when the processing is related to the offering of goods or services to data subjects in the Union;[28] and Article 3(2)(b) applies it to processing activities of controllers and processors without an EU establishment related to the monitoring of the behaviour of data subjects in the EU insofar as such behaviour takes place within the Union.

The GDPR has also been applied by the ECJ to cover cross-border situations that at first glance might seem to fall outside its scope. For example, data processing by Member State intelligence services falls outside the scope of Union law,[29] but they often seek access to data collected by private operators for commercial purposes, which access, as the ECJ has held, is covered by EU law.[30] The Court has also found that the fact that data may be processed by the authorities of a third country for reasons of public security, defence, and State security does not remove it from the scope of the GDPR.[31]

Protection under the rules on territorial scope is supposed to be further strengthened by Article 27(1) GDPR that requires data controllers and processors without an EU establishment whose data processing is subject to the GDPR under Article 3(2) to appoint a representative in the Union, in order "to ensure that the level of protection of data subjects is not reduced where such controllers and processors fail to comply" with the GDPR, and specifically to facilitate enforcement against them.[32] The requirement of appointing a representative thus attempts to compensate for the difficulty of enforcing the GDPR against non-EU data controllers and processors.[33]

27. A data controller determines the purposes and means of processing personal data (Art. 4(7) GDPR), while a data processor processes personal data on behalf of the data controller (Art. 4(8) GDPR).

28. The offering of goods or services to data subjects in the Union involves actions such as designating the EU or a Member State with reference to the good or services; mentioning addresses or phone numbers to be reached from the EU; mentioning a language or currency of a Member State; and others. See EDPB Guidelines 3/2018 cited *supra* note 21, at 17–18.

29. See Consolidated Version of the Treaty on European Union (TEU), Art. 4(2), in particular its last sentence.

30. See e.g. Joined Cases C-511, 512 & 520/18, *La Quadrature du Net et al.*, EU:C:2020:791, and Case 623/17, *Privacy International*, EU:2020:790. See also Docksey, "Schrems II and individual redress –Where there's a will, there's a way", Lawfare (12 Oct. 2020), available at <www.lawfareblog.com/schrems-ii-and-individual-redress-where-theres-will-theres-way>.

31. Case C-311/18, *Data Protection Commissioner* v. *Facebook Ireland Limited and Maximilian Schrems*, EU:C:2020:559 (Grand Chamber) (*Schrems II*), at para 88.

32. Millard and Kamarinou, "Article 27" in Kuner, Bygrave and Docksey (Eds.), *The EU General Data Protection Regulation: A Commentary* (OUP, 2020), pp. 589–598, at p. 590. See also EDPB Guidelines 3/2018 cited *supra* note 21, at 23–28.

33. See COM(2020)264 final, "Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection

2.3. *Data transfer rules*

The data transfer rules contained in Chapter V GDPR will be briefly summarized as they are too lengthy to be quoted here.

Article 44 provides that data transfers are only permissible if all provisions of the GDPR have been complied with before the transfer is carried out, including with regard to further transfers once the data has been sent to the country of destination (so-called "onward transfers"). A legal basis for data transfers may be provided by a formal Commission adequacy decision recognizing that a third country or an international organization[34] provides an adequate level of data protection, which then allows personal data to flow freely to it.[35] An adequacy decision requires that there be a level of protection in the third country that is essentially equivalent to that of EU law, both in theory and in practice.[36] If an adequacy decision is not available, then data transfers may be legalized by the use of "appropriate safeguards", which most frequently involves the use of form contracts approved by the Commission and entered into between data exporters in the EU and data importers outside the EU obligating them to provide protections based on EU law for the data during their transfer and subsequent processing (so-called standard contractual clauses or SCCs).[37] Other forms of appropriate safeguards include legally binding personal data protection policies adopted by a company or other multinational organization established in the EU for data transfers to its group entities (so-called binding corporate rules or BCRs),[38] and approved certification mechanisms,[39] among others.

If an adequacy decision has not been issued and appropriate safeguards cannot be used, it may still be possible to transfer personal data under one of

Regulation", at p. 17, in which the Commission invited the EDPB to "ensure effective enforcement against operators established in third countries falling within the GDPR's territorial scope of application, including as regards the appointment of a representative where applicable (Article 27)".

34. The impact of the GDPR on data transfers to international organizations raises a host of issues under EU law and public international law that will not be dealt with here. See Kuner, "International organizations and the EU General Data Protection Regulation: Exploring the interaction between EU law and international law", 16 *International Organizations Law Review* (2019), 158–191.

35. Art. 45 GDPR.

36. Case C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner*, EU:C:2015: 650 (Grand Chamber), at paras. 73–74.

37. See Art. 46 GDPR.

38. See Arts. 4(20) and 47 GDPR. It should be noted that the term for such measures in Art. 26(2) DPD was "adequate safeguards", but that this was changed to "appropriate safeguards" in Art. 46 GDPR.

39. Art. 46(2)(f).

the derogations (such as when the data subject has consented to the transfer).[40] Derogations are meant to cover situations when there is no adequate protection in the country to which the data is to be transferred, but "the risks to the data subject are relatively small" or "other interests (public interests or those of the data subject himself) override the data subject's right to privacy".[41] They are to be interpreted restrictively[42] and used sparingly. Transfers of personal data may also be legalized by international agreements,[43] although the GDPR does not specify the conditions for this.

2.4. *The text and structure of the GDPR*

The GDPR does not address the relationship between territorial scope and data transfer rules, and the matter seems not to have been considered during the legislative process.[44] This means that nothing in the text of the GDPR suggests that either territorial scope or data transfer rules may not apply just because the other one is applicable. While the two sets of rules have the same underlying policy and thus are complementary, many of the GDPR's provisions are motivated by the same policy,[45] and when it makes one set of protections dependent on another one then this is expressed in the text.[46]

Their standards are also not the same. When data is transferred internationally, they must be processed in a way that satisfies EU standards,[47] but when the GDPR applies to data processing under Article 3(2), it does so regardless of the level of protection in the third country. Data transfer rules mandate that the mechanisms used to provide protection be essentially

40. See Art. 49 GDPR regarding the derogations in general and Art. 49(1)(a) regarding consent.

41. Article 29 Working Party, "Transfers of personal data to third countries: Applying Article 25 and 26 of the EU Data Protection Directive" (WP 12, 24 July 1998), at 24.

42. See e.g. Case C-362/14, *Schrems*, at para 92; Joined Cases C-293 & 594/12, *Digital Rights Ireland*, EU:C:2014:238, at para. 52.

43. Opinion 1/15, *EU-Canada PNR Agreement*, EU:C:2017:592 (Grand Chamber), at para 214.

44. For a detailed discussion of the process for the enactment of the GDPR, see Kuner, Bygrave and Docksey, "Background and evolution of the EU General Data Protection Regulation" in Kuner, Bygrave and Docksey, op. cit. *supra* note 32, pp. 1–47.

45. E.g. transparency of the processing of personal data underlies the provisions of the GDPR relating to the following topics: information given to data subjects (Recitals 39, 58, and 60); rights in automated decision-making (Recital 71); technical and organizational measures (Recital 78); and the establishment of certification mechanisms and data protection seals (Recital 100).

46. E.g. the right to erasure under Art. 17 does not apply in cases involving public interest in the area of public health under Arts. 9(2) and 9(3), see Art. 17(3).

47. See e.g. Case C-362/14, *Schrems*, at para 90; Opinion 1/15, *EU-Canada PNR Agreement*, at paras. 212–215; Case C-311/18, *Schrems II*, at para 184.

equivalent but not necessarily identical to those under EU law,[48] while territorial scope rules result in the application of the GDPR itself. Since the entirety of the GDPR applies to data processing falling within its territorial scope,[49] this means that all of it applies to data processing covered by Article 3. However, the GDPR cannot operate outside the EU exactly as it does within it, since it is based on the EU's legal framework in areas such as the recognition and enforcement of judgments, the rule of law, the independence of the judiciary and the DPAs, and other fundamental rules that by their nature are not addressed to third countries.[50]

The structure of Chapter V also seems to preclude disapplying data transfer rules in cases where the GDPR applies directly. Article 44 creates a link between Chapter V and the rest of the GDPR by providing that data transfers may only take place if all other relevant provisions of the GDPR are satisfied as well. The ECJ has affirmed that transferring personal data to a third country is an act of data processing falling within the scope of the GDPR,[51] so that the rules concerning data transfers must also apply when the GDPR applies. Since all of the GDPR's provisions are applicable to processing falling within its territorial scope,[52] it would seem that a non-EU controller to whom the GDPR is applicable by virtue of Article 3(2) should have to respect all its obligations, including those of Chapter V.[53]

2.5. *The ECJ's requirements of protection*

The rules of the GDPR must be understood in the context of the following requirements for data protection in the international context that the ECJ has set out:

(i) *Data transfers must ensure a high level of protection essentially equivalent to that under EU law*.[54] In *Schrems*,[55] the Court held that a high standard of protection essentially equivalent to that under the

48. Case C-362/14, *Schrems*, at para 73.

49. EDPB Guidelines 3/2018 cited *supra* note 21, at 5.

50. E.g. Art. 36 requires prior consultation with the relevant DPA in certain cases of high-risk data processing, but there are no rules in the GDPR for determining a relevant DPA for non-EU data processing; and many of the powers of DPAs set out in Art. 58 cannot be enforced against parties outside the EU since the enforcement authority of the DPAs ends at the borders of the EU.

51. Case C-311/18, *Schrems II*, at para 83.

52. Ibid.

53. The EDPB admits this, but only with regard to non-EU controllers to which the GDPR applies directly under Art. 3(2), and only for further transfers of data from them to other parties. See 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", at 9.

54. Case C-101/01, *Bodil Lindqvist*, EU:C:2003:596.

Charter and Article 16 TFEU[56] must be applied to Commission adequacy decisions allowing data transfers. It affirmed these conclusions with regard to adequate safeguards such as SCCs in its second *Schrems* decision, referred to here as *Schrems II*.[57]

(ii) *Protection must be effective in practice as well as in law*. Protections must include individuals being able to exercise their rights and having the right to an effective remedy,[58] i.e. there must be effective enforcement.

(iii) *The rationale of these rules is to prevent circumvention of the high level of protection under EU law*. The Court stated in *Schrems* that restrictions on international data transfers are designed to prevent circumvention of the law's high level of protection.[59] Territorial scope rules also aim to prevent the circumvention of EU law by applying the GDPR to data processing that takes places outside EU borders.[60]

(iv) *The territorial scope of EU data protection law as it is currently formulated need not extend in all cases to data processing carried out in a third country; however, such extension is also not prohibited*. In *Google LLC*, the ECJ (Grand Chamber) found that the GDPR does not in its present form require the extension of the right to be forgotten to all the third-country national versions of search engines,[61] but added that the EU legislature could extend the GDPR to cover them if it wanted to,[62] and that courts and DPAs in the Member States were also not prevented from extending the right in this way.[63] Territorial scope was also an issue in *Opinion 1/15*, where the Court required that a draft

55. Case C-362/14, *Schrems*. See Azoulai and Van der Sluis, "Institutionalizing personal data protection in times of global institutional distrust: *Schrems*", 53 CML Rev. (2016), 1343 –1371.

56. Consolidated Version of the Treaty on the Functioning of the European Union (TFEU), O.J. 2012, C 326/47. See Case C-362/14, *Schrems*, at para 40.

57. Case C-311/18, *Schrems II*, at para 96.

58. See Case C-362/14, *Schrems*, at paras. 64–65, 73–74, and 95; Opinion 1/15, *EU-Canada PNR Agreement*, at para 220; Case C-311/18, *Schrems II*, at paras. 105 and 187.

59. Case C-362/14, *Schrems*, at para 73.

60. See Recital 23 GDPR, explaining the rationale of the rules of Art. 3(2) as being "In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation …".

61. Case C-507/17, *Google LLC*, EU:C:2019:772, at paras. 61–65. Supporting this view, see Gömann, *Das öffentlich-rechtliche Binnenkollisionsrecht der DS-GVO* (Mohr Siebeck, 2021), pp. 563–565.

62. Case C-507/17, *Google LLC*, at para 58.

63. Ibid., at para 72. See also Opinion of A.G. Szpunar in Case C-507/17, *Google Inc.* v. *Commission nationale de l'informatique et des libertés (CNIL)*, EU:C:2019:15, para 53, stating that extraterritorial effects are accepted as a basis for jurisdiction in EU law only in "extreme situations of an exceptional nature".

international agreement with Canada limit onward transfers to other countries of EU data sent to Canada under the agreement.[64]

(v) *Data protection concepts should be interpreted broadly so that individuals are not deprived of complete and effective protection*. In its judgments concerning the international processing of data, the ECJ has required that a consistent and homogenous application of the Charter be ensured[65] and that circumvention of protections be avoided.[66] This requires that important concepts of data protection law be interpreted broadly in order to avoid gaps in protection or situations where there is no party to which individuals can turn to assert their rights. For example, in both its *Google Spain*[67] and *Wirtschaftsakademie*[68] judgments, the Court interpreted the concept of data controller broadly in an international context in order to avoid circumvention of the law. This is in effect a corollary of the principle of accountability discussed below.

2.6. *Issues and questions*

The preceding discussion explains how the GDPR seeks to protect EU personal data through the use of territorial scope and data transfer rules. In order to understand the relationship between the two sets of rules, it is necessary to view their interaction systematically, in light of the issues they present. The standard for such an evaluation is provided by Article 7 TFEU, which requires that there be consistency between the EU's policies and activities taking all of its objectives into account, and that duplications and contradictions between Union measures be avoided.[69] The consistency of the measures is closely connected with their effectiveness in protecting EU data, since inconsistent measures are likely to be inefficient, ineffective, and leave gaps in protection. The consistency of the GDPR's protections against external threats to data can be evaluated based on the following three factors.

64. See Opinion 1/15, *EU-Canada PNR Agreement*, at paras. 212–217. The coverage of onward transfers also follows from Art. 44 GDPR. See Kuner, "International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, *EU-Canada PNR*", 55 CML Rev. (2018), 857–882.

65. Case C-311/18, *Schrems II*, at para 101.

66. Case C-131/12, *Google Spain SL*, at paras. 54 and 58.

67. Ibid., at paras. 34–41.

68. Case C-210/16, *Unabhängiges Zentrum für Datenschutz Schleswig-Holstein* v. *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388, at paras. 28–44.

69. See Klamert, "Article 7 TFEU" in Kellerbauer, Klamert and Tomkin (Eds.), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (OUP, 2019), pp. 380–382, at p. 381.

First, the same rules could apply to the same data processing in a way that produces conflicts or duplications between them, i.e. they could *overlap*. That both sets of rules may apply to the same data processing is shown by the fact that although the two *Schrems* judgments of the ECJ dealt with Facebook's data transfer practices, courts in the EU have also found that Facebook makes use of plug-ins and cookies to track and identify users, and that this processing falls under the territorial scope of EU data protection law.[70] In addition, the GDPR mentions audits of data processing being performed by the data controller or data protection officer,[71] and data transfer mechanisms may also require data controllers to conduct audits.[72] However, not every duplication of protections results in inconsistency, and its effects must be judged in each particular case. It is common in the GDPR for different protections to be motivated by the same underlying policy; for example, the appointment of a data protection officer is designed to identify and mitigate risks to data processing,[73] which is also one of the purposes of data security measures.[74] Thus, rules concerning audits set out in data transfer mechanisms are concretizations of the relevant rules of the GDPR, so that they may not necessarily produce inconsistent obligations. Moreover, individuals may welcome their data being subject to multiple protections.

A second factor could be a *lack of standards* for coordinating which set of rules apply. For example, the GDPR contains principles relating to data processing in Article 5, which are also contained in the SCCs approved by the Commission.[75] However, this does not present a problem, since the principles in the SCCs were drafted based on those contained in the GDPR. As will be seen below, the EDPB and the Commission have taken positions on the interaction of the two sets of rules, but both are open to criticism, and it would be preferable to have this matter clarified in the text of the GDPR itself or by the ECJ.

70. See regarding such a judgment in Belgium, Ducuing, "Cookies and other (illegal) recipes to track internet-users: Latest episode of the Facebook saga", KU Leuven Centre for IT & IP Law, available at <www.law.kuleuven.be/citip/blog/cookies-and-other-illegal-recipes-to-track-internet-users-latest-episode-of-the-facebook-saga/>.

71. See Art. 28(3)(h), Art. 39(1)(b), and Art. 47(2)(j) GDPR.

72. See e.g. Agencia Española de Protección de Datos, "Approval of binding corporate rules of Fujikura Automotive Europe Group (FAE Group)", available at <edpb.europa.eu/sites/default/files/bcr_decision_sa/es_final_decision_bcr_grupo_fae_2020_en.pdf>, at 3, requiring Fujikura to conduct data protection audits.

73. Recital 77 GDPR.

74. Recital 83 GDPR.

75. 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, O.J. 2021, L 199/31, Clause 8.

A third factor could be the creation of *gaps in protection*, such as when the rules interact so that protection does not apply in certain data processing situations. This is the case at present with regard to enforcement of the GDPR, since the EDPB and the Commission have prioritized its direct application over data transfer rules in certain circumstances, even though the GDPR lacks some of the enforcement possibilities contained in data transfer mechanisms, as will be discussed below.

The consistency of Union legal measures cannot be determined with mathematical precision, and it is a concept that seems to be under-analysed.[76] However, evaluating initiatives taken by the EDPB and the Commission in light of the factors discussed above and the important principles of accountability, ensuring a high level of protection, and effective enforcement shows that they do not adequately consider the respective rationales and roles of territorial scope and data transfer rules. As a result, there is a risk that the protections of the GDPR may be undermined and its global influence reduced. Thus, it is important that EU bodies interpret the two sets of rules in a way that upholds each of these principles and maintains a high level of protection.

3. Initiatives of EU bodies

3.1. *Introduction*

EU bodies have struggled to interpret territorial scope and data transfer rules in a consistent fashion, as can be seen in initiatives of the EDPB and the European Commission.

3.2. *Guidelines of the European Data Protection Board*

The EDPB addressed the interplay between territorial scope and data transfer rules for the first time in an unpublished draft of its Guidelines 3/2018 on the territorial scope of the GDPR under Article 3 dated 14 September 2018 (the "EDPB unpublished draft"),[77] where it found that Chapter V should not apply in cases where the GDPR applies to data processing under Article 3 directly. The unpublished draft stated that Chapter V compensates for the protection given to data when the GDPR applies under Article 3, and that the relationship of the two provisions can thus be described as "complementary or

76. See Dawson, "Better regulation and the future of EU law and politics", 53 CML Rev. (2016), 1209–1236, at 1227.

77. EDPB, "Guidelines on the territorial scope of the GDPR (Article 3)", v 0.5 (unpublished draft, on file with the author).

compensatory".[78] Thus, it was stated, "when the processing of personal data carried out by the data recipient (controller or processor) in a third country is covered by the scope of the GDPR in accordance with Article 3, there is no lack of protection and Chapter V shall not apply to the passing of the data to the data recipient".[79] This language was not included in the final version of the guidelines issued in November 2019,[80] which had been preceded by a consultation version.[81] The final version includes only a few brief references to Chapter V, and states that the EDPB "will also further assess the interplay between the application of the territorial scope of the GDPR as per Article 3 and the provisions on international data transfers as per Chapter V. Additional guidance may be issued in this regard, should this be necessary."[82]

In November 2021, the EDPB then adopted a public consultation version of its Guidelines 05/2021 (the "Guidelines")[83] specifically dealing with the interplay between territorial scope and data transfer rules. The Guidelines include for the first time a definition of international data transfer, which requires that there be: 1) a controller or processor subject to the GDPR for the given processing; 2) disclosure of the data or making them available by this party to another controller or processor; and 3) a data importer that is located in a third country or that is an international organization.[84] The Guidelines conclude that an international data transfer does not exist "where the data are disclosed directly and on his/her own initiative by the data subject",[85] since "in such case, there is no controller or processor sending or making the data available ('exporter')".[86] The EDPB bases its definition of international data transfer on the ECJ's *Lindqvist* judgment from 2003.[87] This position in effect grants priority to the direct application of the GDPR by defining data transfers to exclude many situations where individuals themselves transmit their own data to non-EU websites.

The EDPB has issued a call for consultation on the Guidelines 05/2021,[88] but had not issued a further version of them at the time this article was finalized. Based on prior experience with EDPB consultations, their

78. Ibid., at 24.
79. Ibid., at 23–24.
80. EDPB Guidelines 3/2018 cited *supra* note 21.
81. EDPB, "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation".
82. EDPB Guidelines 3/2018 cited *supra* note 21, at 22.
83. EDPB Guidelines 05/2021 cited *supra* note 53.
84. Ibid., at 4.
85. Ibid., at 5.
86. Ibid.
87. Ibid., at 4.
88. See <edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en>.

substance seems unlikely to change significantly in the final version, and even if some changes are made, the consultation version demonstrates the major elements of the EDPB's view.

3.3. *Decisions of the European Commission*

The Commission's view of the relationship between territorial scope and data transfer rules has evolved over time. In the years following adoption of the DPD, it seemed to view data collection via the Internet by non-EU parties as a form of data transfer. This can be seen in an unpublished Commission document from 2001 which refers to the collection and further processing of personal data in the EU using the Internet as "an important means of transfer", and states that data collection by a company actively seeking customers in the EU by means of the Internet would involve "an individual transferring his own data" to the company.[89] The conflation of the two sets of rules can also be seen in the Commission's statement when proposing the GDPR in 2012 that "individuals' rights must continue to be ensured when personal data is transferred from the EU/EEA to third countries, and whenever individuals in Member States are targeted and their data is used or analysed by third-country service providers".[90]

In its review of the first two years of application of the GDPR, the Commission stated that "several submissions to the public consultation" mentioned the need to re-examine the rules when parties conducting data transfers are also covered by the GDPR.[91] However, an examination of the 129 submissions the Commission received to the public consultation on the GDPR[92] reveals only one that mentions the interaction between Article 3 and Chapter V specifically, and then only briefly,[93] indicating that the Commission's attention to this question is more likely the result of an internal decision than of public pressure.

The SCCs that the Commission issued in 2021, which include both an implementing decision and the set of SCCs as an annex, may be used for transfers to processors and controllers established in third countries "only to

89. European Commission, Internal Market DG, "Protection of personal data: Impact of Directive 95/46/EC on transfers to third countries", at 7 (Nov. 2001, unpublished paper, on file with the author).

90. Commission Communication cited *supra* note 25, at 10.

91. Commission Staff Working Document . . . Accompanying the Document Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, SWD(2020)115 final, at 31 note 114.

92. See <ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Data-protection-report-on-the-General-Data-Protection-Regulation_en>.

93. Ibid., Feedback from Sky, at p. 2.

the extent that the processing by the importer does not fall within the scope of Regulation (EU) 2016/679".[94] This means that the SCCs may not be used for data transfers to parties whose processing of data falls under the GDPR.[95] This is a departure from the previous sets of SCCs the Commission approved under the DPD, which did not contain such limitation.[96] The Commission has justified the SCCs not being available for data transfers to parties subject to the GDPR by stating that "this would duplicate and, in part, deviate from the obligations that already follow directly from the GDPR".[97] However, the Commission goes on to state that it is "in the process of developing an additional set of SCCs for this scenario";[98] this is discussed further below.

Recent adequacy decisions issued by the Commission state that they do not affect the direct application of the GDPR,[99] implying that both direct application of the GDPR and data transfers made under adequacy decisions can co-exist. However, the Commission has indicated that it is likely to insert language in adequacy decisions mirroring that used in the SCCs, i.e. indications that an adequacy decision does not apply to transfers to a data importer whose processing of the data is directly subject to the GDPR.[100]

The fact that the Commission has failed to provide an explanation for its view of the relationship between territorial scope and data transfer rules in its

94. Commission Implementing Decision cited *supra* note 75, Recital 7. See also, ibid, Art. 1(1), stating that "The standard contractual clauses set out in the Annex are considered to provide appropriate safeguards within the meaning of Article 46(1) and (2)(c) of Regulation (EU) 2016/679 for the transfer of personal data from a controller or processor subject to Regulation (EU) 2016/679 (data exporter) to a controller or (sub) processor *not subject to Regulation (EU) 2016/679 (data importer)*" (emphasis added).

95. European Commission, "The New Standard Contractual Clauses – Questions and Answers" (25 May 2022), at 13.

96. See e.g. Commission, Decision (EC) 2001/497 of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive (EC) 95/46, O.J. 2001, L 181/19, and Commission Decision (EC) 2010/87/EU of 5 Feb. 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive (EC) 95/46/EC of the European Parliament and of the Council, O.J. 2010, L 39/5.

97. European Commission Q&A cited *supra* note 95, at 13–14.

98. Ibid., at 14.

99. Commission Implementing Decision of 17 Dec. 2021 pursuant to Regulation (EU) 201 6/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Data Protection Act, Recital 7; Commission Implementing Decision (EU) 2019/419 of 23 Jan. 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, O.J. 2019, L 76/1, Recital 5; Commission Implementing Decision of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, O.J. 2021, L 360/1, Recital 7.

100. Informal communication from the European Commission.

formal decisions seems problematic under the TFEU, which requires the Commission to give reasons for its decisions.[101] This obligation is particularly important in an area such as data protection which concerns EU fundamental rights.

4. Important principles of protection

4.1. *Introduction*

These initiatives of the EDPB and the European Commission raise questions about whether they are compatible with standards of protection set out in the GDPR and affirmed by the ECJ. In particular, the principle of accountability, the need for a high level of protection, and effective enforcement, may be undermined by these actions. By leading to gaps in protection, the initiatives and interpretations of EU bodies risk creating inconsistency with the high standard of data protection required under EU law.

4.2. *Accountability*

The GDPR requires that data controllers be accountable for their actions, i.e. that parties processing personal data have a proactive obligation to adopt appropriate measures to protect them and to be able to demonstrate compliance.[102] This is expressed in the GDPR itself,[103] and has been affirmed by the Court in its judgments[104] and by President Lenaerts, who has referred to the Court's attachment to "high levels of accountability" of parties processing personal data.[105] Thus, as Docksey states, "the concept of accountability lies at the root of the new approach to compliance demanded by the GDPR".[106]

101. See Art. 2 of Protocol 2 on the Application of the Principles of Subsidiarity and Proportionality, O.J. 2004, C 310/207; see also Dawson op. cit. *supra* note 76, 1218–1223.

102. See Docksey, "Article 24" in Kuner, Bygrave and Docksey, op. cit. *supra* note 32, pp. 555–570, at p. 566.

103. See e.g. Arts. 5(2) and 24 GDPR.

104. See e.g. Case C-210/16, *Wirtschaftsakademie*, at para 28; Case C-25/17, *Jehovan todistajat*, EU:C:2018:551, at para 66. See also Docksey, op. cit. *supra* note 102, at 566–568.

105. Lenaerts, "The EU General Data Protection Regulation five months on", speech by ECJ President Koen Lenaerts at the 40th International Conference of Data Protection and Privacy Commissioners (25 Oct. 2018), available at <www.youtube.com/watch?v=fZaKPaGbXNg>. See also Docksey and Hijmans, "The Court of Justice as a key player in privacy and data protection: An overview of recent trends in case law at the start of a new era of data protection law", 5 *European Data Protection Law Review* (2019), 300–316.

106. Docksey, op. cit. *supra* note 102, at p. 568.

Accountability also applies to the processing or transfer of EU data beyond EU borders, as the EDPB has found.[107]

Accountability is undermined by the EDPB's definition of international data transfers, according to which there will be no data controller to whom individuals can turn when they send their personal data to a non-EU party. The ECJ has held that "the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data",[108] and has required that the concept of "data controller" be given a broad definition in order to ensure effective and complete protection.[109] This would seem to require that it be interpreted broadly in the context of international data transfers as well.

However, under the EDPB's definition of data transfer, neither individuals who enter their personal data on Internet sites nor the operators of non-EU websites, whether or not they engage in offering goods or services to EU individuals or online profiling, are considered to be data controllers, so that such data entry falls into a legal "no man's land" without any party being responsible for complying with obligations related to the data being transferred outside the EU. For example, information about the risks of transfers or the safeguards used must be provided by the data controller under Articles 13(1)(f), 14(1)(f), 15(2), and Article 49(1)(a) GDPR when a data transfer occurs, but if the entry by an individual of their own data on a website is deemed not to be a data transfer, then the party operating the website will not be responsible for providing such information, which seems to result in a situation where no accountability exists. As the Commission already recognized in its paper from 2001 quoted above,[110] the entry of data onto a website effectively results in its being transferred to the party in control of the website; any attempt to distinguish data entry from data transfer in this situation is linguistic sophistry.

4.3. *Ensuring a high level of protection*

The ECJ requires that EU data receive a high level of protection also when they are processed in or transferred to third countries. Thus, any interpretation or implementation of the rules of Article 3 and Chapter V must meet this

107. EDPB, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", Version 2.0, at 3.

108. Case C-362/14, *Schrems*, at para 45.

109. Case C-210/16, *Wirtschaftsakademie*, at para 28. See also Docksey, op. cit. *supra* note 102, at p. 566.

110. See European Commission unpublished paper cited *supra* note 89.

standard, but it is questionable whether the recent initiatives of the EDPB and the Commission do so.

The EDPB definition of international data transfer is based solely on the ECJ's *Lindqvist* judgment from 2003,[111] although the Court's holding in that case was limited to determining that the upload of data to a website stored with a hosting provider established in the EU did not constitute an international data transfer under the former DPD.[112] Moreover, it was decided before the Charter of Fundamental Rights was raised to the status of primary law in 2009,[113] and since then the ECJ has relied on the Charter to emphasize the need for a high standard of protection for international data transfers in the context of international agreements of the EU,[114] Commission adequacy decisions,[115] and the EU standard contractual clauses.[116] In light of these judgments, any definition of international data transfers should be based on the necessity of providing a high level of protection, not on a single judgment decided many years ago under a different legal framework. This would also seem to be required by the approach that the ECJ takes in cases involving the fundamental right to data protection, under which the Court makes a "dynamic assessment" and evaluates whether they meet the legal standards in force at the time that it decides its judgments and not just those that applied when the case was brought.[117]

The EDPB definition is also logically inconsistent. It recognizes that parties to whom the GDPR applies under Article 3(2) must comply with data transfer requirements if they transfer the data received from the EU further to other parties,[118] but not does require that they themselves comply with Chapter V as data importers when receiving the data. In addition, if such a party does not engage in offering goods or services to EU individuals or monitoring their behaviour, it will not fall under Article 3 at all and the data processing will also not receive protection under Chapter V. Any definition that results in a common data transfer scenario such as the entry of data onto non-EU websites not falling under the data transfer rules cannot result in a high level of protection.

The actions of the EDPB and the Commission also undermine the level of protection by encouraging online monitoring. If falling under Article 3 removes the need to implement a data transfer mechanism, then non-EU

111. EDPB Guidelines 05/2021 cited *supra* note 53, at 4.
112. Case C-101/01, *Bodil Lindqvist*, at para 71.
113. Art. 6(1) TEU.
114. Opinion 1/15, *EU-Canada PNR Agreement*, at paras. 119–231.
115. Case C-362/14, *Schrems*, at paras. 38–40.
116. Case C-311/18, *Schrems II*, at para 99.
117. See speech cited *supra* note 105, between 27'07" and 30'35".
118. EDPB Guidelines 05/2021 cited *supra* note 53, at 9.

entities would only have to begin monitoring EU individuals to avoid using one. Discouraging such monitoring was an important goal of the GDPR,[119] and finding that data transfer rules do not apply to direct online interactions of websites with data subjects contradicts this policy. The ECJ has held that "the Commission's discretion as to the adequacy of protection ensured by a third country is reduced", and its review of such adequacy "should be strict",[120] which cannot be consistent with incentivizing online monitoring by non-EU websites.

4.4. *Effective enforcement*

The ECJ requires that data protection be effective in practice, which means that there must be effective redress mechanisms and judicial remedies against violations of the GDPR,[121] i.e. that there must be effective enforcement of the law. Data transfer rules contain mechanisms that help compensate for the difficulty of enforcing obligations under EU law against parties in third countries. For example, when issuing an adequacy decision the Commission must ensure that data protection in the third country provides for "effective and enforceable data subject rights and effective administrative and judicial redress"[122] and that there is an independent supervisory authority with "adequate enforcement powers".[123] This is the reason that the SCCs contain clauses giving data subjects extra redress mechanisms against data importers;[124] that BCRs must ensure effective enforcement, such as acceptance by the EU controller or processor of liability for breaches by non-EU members of the corporate group[125] and the use of audit and verification procedures;[126] and that certification mechanisms used as a legal basis for data transfers must contain enforceable commitments such as contractual guarantees.[127] Many protections that apply under data transfer rules can also be enforced against the data exporter in the EU.[128]

119. See Recital 24 GDPR; Hustinx, "EU data protection law: The review of Directive 95/46/EC and the General Data Protection Regulation" in Cremona (Ed.), *New Technologies and EU Law* (OUP, 2017), pp. 123–173, at pp. 124 and 155.
120. Case C-362/14, *Schrems*, at para 78.
121. See e.g. Case C-311/18, *Schrems II*, at paras. 186–189.
122. Art. 45(2)(a) GDPR.
123. Art. 45(2)(b) GDPR.
124. See e.g. European Commission, Annex to the Commission Implementing Decision 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 O.J. 2021, L 199/31, Clauses 10–11.
125. Art. 47(2)(f) GDPR.
126. Art. 47(2)(j) GDPR.
127. EDPB, "Guidelines 07/2022 on certification as a tool for transfers", at 16.
128. See e.g. European Commission Annex cited *supra* note 124, at Clause 2.

By contrast, when the GDPR applies directly to data processing in a third country, it does so regardless of the possibility of enforcement. The GDPR grants individuals the right to lodge a complaint with a DPA (Art. 77) or a court (Art. 79) in the EU when it applies directly to a party outside the EU. This is likely to be ineffective, however, unless the non-EU party has an EU establishment, because the enforcement powers of the DPAs end at EU borders,[129] and it is expensive and difficult to have court judgments or DPA decisions recognized and enforced in third countries. The appointment of a representative by non-EU parties subject to the GDPR under Article 3(2) hardly makes a significant contribution to effective enforcement, as the representative's liability is limited to violations of its own direct obligations under Article 30 and Article 58(1)(a) GDPR[130] and does not substitute for that of the data controller or data processor it represents.[131] All this leads to the conclusion that the application of the GDPR under Article 3(2) is designed to put non-EU actors on notice that manipulating the data of EU individuals has legal consequences rather than to threaten a high risk of legal enforcement.[132]

The EDPB Guidelines attempt to address this enforcement deficit by suggesting that new SCCs be developed "in cases where the importer is subject to the GDPR for the given processing in accordance with Article 3(2)";[133] as mentioned above, the Commission has also committed to develop such contractual clauses.[134] However, this does not seem to make sense, since under the EDPB's own definition of data transfer, in such cases "there is no controller or processor sending or making the data available"[135] (i.e. no data exporter) and thus no party for the data importer to sign the SCCs with.

The ineffectiveness of relying on Article 3(2) GDPR to protect data processed outside the EU is likely one of the reasons this provision is seldom used in practice as the sole legal basis for enforcement action against non-EU data controllers and processors. Instead, Article 3(1) is used when applicable, with Article 3(2) sometimes added as an afterthought.[136] This can be seen in the *Wirtschaftsakademie* case of the ECJ, where the Opinion of Advocate General Bot indicates that online monitoring via cookies was being carried out

129. Case C-362/14, *Schrems*, at para 44.

130. EDPB Guidelines 3/2018 cited *supra* note 21, at 28.

131. Ibid., at 27.

132. Svantesson refers to this type of jurisdiction as "bark" jurisdiction, defined as an attempt to make clear or articulate a particular legal position (as opposed to "bite" jurisdiction, defined as being aimed at effective enforcement). See Svantesson, "A jurisprudential justification for extraterritoriality in (private) international law", 13 *Santa Clara Journal of International Law* (2015), 517–571, at 556–566.

133. EDPB Guidelines 05/2021 cited *supra* note 53, at 9.

134. See European Commission Q&A cited *supra* note 95, at 14.

135. Ibid., at 5.

136. See Gömann, op. cit. *supra* note 61, at pp. 561–568.

by Facebook in the US (i.e. under Art. 4(1)(c) DPD or Art. 3(2) GDPR), but jurisdiction was founded against Facebook's European establishments based on the fact that it was inextricably linked with such activity (i.e. under Art. 4(1)(a) DPD or Art. 3(1) GDPR).[137]

Relying solely on territorial scope rules under Article 3 to enforce the GDPR also raises a number of practical problems. There are untold millions of companies outside the EU that lack an EU establishment, but that interact with EU individuals via the Internet, and thus may be subject to direct application of the GDPR only under Article 3(2) (i.e. by offering goods or services online to such individuals or monitoring their behaviour). For the reasons described above, there will be little possibility of legal enforcement against such entities, in effect leaving individuals without a remedy when their data is processed by websites without an EU establishment. If such a party has concluded the SCCs, the Commission's view will allow it to escape from its obligations under them by arguing that actually it is subject to the GDPR under Article 3(2), thus rendering moot any enforcement action under the SCCs. This allows for manipulation of the legal basis for enforcement actions, and puts the burden of determining whether a non-EU party is subject to the GDPR on individuals seeking to assert their rights before a court or a DPA. The lack of clarity about when data processing falls under Article 3(2)[138] will also likely lead to confusion on the part of non-EU parties as to which rules apply when they receive EU data.

5. Implications for the GDPR's global influence

The EU has attempted to establish the GDPR as a global standard of data protection.[139] Doing so strengthens the protection of data processed outside the EU's borders, since the more the law of third countries resembles EU data protection law, the less the risk that the EU's own standards will be circumvented. It has been quite successful in this regard, with 145 countries having enacted data protection laws based on the EU model according to one

137. Opinion in Case C-210/16, *Unabhängiges Zentrum für Datenschutz Schleswig-Holstein* v. *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2017:796, at para 81.

138. See Svantesson in Kuner, Bygrave and Docksey, op. cit. *supra* note 32, at pp. 88–91, criticizing the rules of Art. 3(2) as unclear.

139. See e.g. the remarks of former EU Commissioner Viviane Reding, "A data protection compact for Europe" (28 Jan. 2014), available at <europa.eu/rapid/press-release_SPEECH-14-62_en.htm>; and former Rapporteur of the European Parliament Jan-Philipp Albrecht, "How the GDPR will change the world", 3 *European Data Protection Law Review* (2016), 287–289, at 287.

count.[140] The continuing global influence of the GDPR is also shown by the Executive Order issued by US President Biden in October 2022 referred to above.

Protections that apply to data processing and data transfers outside the EU, such as adequacy decisions and SCCs, are one of the main mechanisms by which the GDPR's global influence is exercised, since they make the processing of personal data in third countries or their transfer to them conditional on the application of EU standards.[141] The Commission has also adopted a standard text on cross-border data flows and the protection of personal data and privacy that it seeks to incorporate into the EU's trade agreements.[142] The relationship between the EU's efforts to establish the GDPR as a global standard and its data transfer rules can be seen in a letter the Commission sent to the EDPB in June 2021, stating that if the latter did not take a more positive view of the Commission's adequacy decisions for the UK,[143] this would "show that our model is not credible as a global solution".[144]

The global influence of the GDPR means that many third countries need to keep their data protection standards closely aligned with those of the EU, either for legal reasons (i.e. because they have obtained a favourable adequacy decision from the Commission, or hope to) or because of economic or political considerations. Such alignment also benefits the EU, as it lowers the risk of circumvention of EU law when data is processed in or transferred to a third country. Thus, the impact on third countries of the EU's standards can influence the protection provided to EU data as well, either to its advantage (if they stay close to EU standards) or its disadvantage (if they do not).

140. See Greenleaf, "Global data privacy laws 2021: Despite COVID delays, 145 laws show EU dominance", available at <papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348>.

141. See e.g. Kuner, op. cit. *supra* note 10, at 125–126; Mills, "Private international law and EU external relations: Think local act global, or think global act local?", 65 ICLQ (2016), 541–579, at 573–574.

142. European Commission, "EU proposal for provisions on cross-border data flows and protection of personal data and privacy", available at <trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf>. See also Yakovleva and Irion, "Pitching trade against privacy: Reconciling EU governance of personal data flows with international trade", 10 *International Data Privacy Law* (2020), 201–221, at 219–220.

143. The UK left the EU on 31 Jan. 2020 (Brexit). The Commission has adopted adequacy decisions covering respectively data transfers to the UK under the GDPR (Commission Implementing Decision of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, cited *supra* note 99 and the Law Enforcement Directive (Commission Implementing Decision of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021)4801 final).

144. Manancourt, "Why Brussels went easy on Britain on its data deal", POLITICO (30 June 2021), available at <www.politico.eu/article/why-brussels-went-easy-on-britain-in-data-adequacy-deal/>.

The way that the GDPR's protections against external threats are interpreted and implemented thus affects the global reach of EU data protection law. The more consistency the GDPR's protections demonstrate, the greater its influence in third countries. This also creates a virtuous circle by motivating more third countries to adopt the standard of the GDPR, which in turn increases the protection given to EU data by aligning third country standards to those of the EU. However, the reverse is also true: the more inconsistent the GDPR's standards appear, the less the motivation to adopt them, and the less third-country standards will resemble those of EU law.

6. Achieving cross-border data protection

6.1. *Introduction*

The similar rationale of territorial scope and data transfer rules combined with the lack of clarity concerning their interaction has led to inconsistency in the protection against external threats under the GDPR. While overlap between territorial scope and data transfer rules may occur, it is not clear whether this presents a problem: no specific issues caused by it have been identified, and it would seem that any conflicts could be resolved by applying the rule that is more protective to individuals, as the ECJ requires.[145] There are also no standards for determining how the two sets of rules interact, which creates confusion. And the way that EU bodies have dealt with their interaction risks creating gaps in protection.

It also seems that they have been interpreted without regard to any underlying rationale, which further supports the conclusion that they are applied inconsistently. For instance, the Commission has stated that the GDPR does not apply to data processing by international organizations under public international law and that data can only be transferred to them if one of the data transfer mechanisms set out in Chapter V is used.[146] This is the opposite position to that taken by both the EDPB and the Commission with regard to territorial scope and data transfer rules in general. Giving priority to data transfer mechanisms that have been designed to provide protections tailor-made for the risks of the international environment and which provide stronger possibilities of enforcement would better meet the standard set by the

145. See e.g. Case C-40/17, *Fashion ID GmbH & Co. KG*, EU:C:2019:629, at para 50.
146. See Kuner, op. cit. *supra* note 34, at 170 and 182.

ECJ that data protection in the international context must be "effective and complete",[147] which requirement it said cannot be interpreted restrictively.[148]

Such inconsistency can only be resolved if EU bodies interpret and implement the GDPR's rules on territorial scope and data transfers in a way that preserves accountability and ensures effective protection against external threats. Each body has an important role to play in this regard, as described below.

6.2. *The role of the ECJ*

As the ultimate arbiter of EU law, the ECJ determines how protections under the GDPR should be applied. While it has interpreted both territorial scope and data transfer rules broadly and emphasized their importance for ensuring a high level of protection, it has sometimes created confusion by applying one set of rules but not the other for reasons that are not clear. For example, in his Opinion in *Google Spain*, Advocate General Jääskinen accepted Google's assertion that it did not use cookies,[149] although Google's web pages confirm that it uses them in its services.[150] Neither he nor the Court in its judgment examined whether the DPD would apply based on Google's use of equipment (i.e. cookies) under Article 4(1)(c) despite the fact that this was among the questions referred to it by the Spanish court.[151] The issue of international transfers of data to the Google search engine was also not examined in either the Opinion or the judgment, even though Google's web pages confirm that it transfers "online advertisement and measurement personal data" from the EEA using the SCCs.[152] Similarly, in *Wirtschaftsakademie* the Opinion of Advocate General Bot indicated that online monitoring via cookies was being carried out by Facebook in the US[153] and that data was being transferred to the

147. Case C-131/12, *Google Spain SL*, at para 34. See Docksey and Hijmans, "The Court of Justice as a key player in privacy and data protection", 3 *European Data Protection Law Review* (2019), 300–316, at 304.

148. Case C-131/12, *Google Spain SL*, at para 53.

149. Opinion in Case C-131/12, *Google Spain SL, Google Inc* v. *Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, EU:C:2013:424, at para 62.

150. See Google, "How Google uses cookies", available at <policies.google.com/technologies/cookies?hl=en-US>, mentioning among other uses of cookies that "Some cookies improve the performance of Google services. For example, 'CGIC' improves the delivery of search results by autocompleting search queries based on a user's initial input. This cookie lasts for 6 months."

151. See Case C-131/12, *Google Spain*, at para 20, questions 1(b)-(d).

152. See Google, "Update to Standard Contractual Clauses (SCCs)" (Aug. 2020), available at <support.google.com/adspolicy/answer/10042247?hl=en>.

153. Opinion in Case C-210/16, *Wirtschaftsakademie*, at para 81.

servers of the US Facebook parent.[154] However, neither of these issues was mentioned in the Court's judgment. And in his Opinion in *Schrems II*,[155] Advocate General Saugmandsgaard Øe distinguished between "processing consisting in the transfer itself" and subsequent data processing by national security authorities of a third country, finding that the latter was excluded from the territorial scope of the GDPR.[156] However, the Court did not mention this point in its judgment.

The failure to discuss these issues may be explained by the fact that they are not mentioned in the questions referred to the Court, or that it may not have had to deal with them in light of other conclusions it drew.[157] However, the Court often reworks or reformulates the questions referred to it before answering them,[158] and has the "duty to interpret all provisions of Union law which the national court needs to decide the case pending before it, even if those provisions are not expressly indicated in the questions".[159] Thus, there is nothing preventing the Court from clarifying the relationship between Article 3 and Chapter V if a case is referred to it which presents issues arising under both sets of provisions.

It is also important that a crucial term such as "international data transfer" be defined not just by the EDPB, but by the Court, and that it adopt a definition meeting the standard it set when stating that the concept of data controller should be defined "to ensure . . . effective and complete protection of data subjects".[160] A non-EU party that provides a website by means of which an EU individual's data is processed in a third country should be regarded as a controller that initiates a data transfer, since the data is being collected and processed for its own interests via means that it has created and controls. While not all data transfer mechanisms could be implemented in such situations (e.g. individuals could not sign SCCs as exporters of their own data), the website controller could be expected to implement one of the mechanisms that are feasible in such situations: for example, joining an approved code of conduct or certification mechanism under Article 46(2) and complying with other relevant requirements of the GDPR such as

154. Ibid., at para 50.

155. Opinion in Case C-311/18, *Data Protection Commissioner* v. *Facebook Ireland Limited and Maximilian Schrems*, EU:C:2019:1145.

156. Ibid., at para 104.

157. E.g. in *Google Spain*, the ECJ found that there was no need to examine the application of Art. 4(1)(c) of the DPD since it had found that the DPD applied based on there being establishments of Google in a Member State under Art. 4(1)(a). See Case C-131/12, *Google Spain*, at para 61.

158. See Lenaerts, Maselis and Gutman, *EU Procedural Law* (OUP, 2014), Kindle edition, location 15579.

159. Ibid.

160. Case C-131/12, *Google Spain*, at para 34.

informational obligations. Any other interpretation will allow data transfers to be carried out without any party being responsible for them and will reduce the level of protection that personal data receives.

6.3. *The role of the EDPB*

Article 70(1)(e) GDPR gives the EDPB the power to "issue guidelines, recommendations and best practices" in order to ensure consistent application of the GDPR. However, this should not result in its positions on issues of fundamental importance being regarded as definitive when clarification of them by the ECJ or the legislature is needed. Moreover, the EDPB should explain its reasoning and the basis for its positions in light of ECJ judgments emphasizing the need for a high standard of protection.

6.4. *The role of the Commission*

The Commission issues decisions on the adequacy of protection in third countries and appropriate safeguards that determine how the protections of the GDPR are applied in practice. Its power to adopt implementing acts such as adequacy decisions and SCCs, however, is subject to the restrictions of Article 291 TFEU under which it may not amend or supplement the underlying legislative act.[161] Defining the interaction of Article 3 and Chapter V so that the latter does not apply to data importers subject to the GDPR when there is no indication of this in the text or policy of the GDPR, seems to come perilously close to violating this standard. Like the EDPB, the Commission should also be more transparent in explaining its reasoning for adopting positions with such far-reaching implications.

Concretely, this means that the Commission should avoid confusion about the relationship between territorial scope and data transfer rules, and ensure that its formulations do not undermine the GDPR's protections. It is obliged to evaluate the GDPR every four years,[162] in particular the rules on international data transfers,[163] and, if necessary, propose amendments to it.[164] In light of the uncertainties surrounding the interaction of these two sets of rules, the Commission should propose that the concept of international data transfer be

161. Case 65/13, *European Parliament* v. *Commission*, EU:C:2014:2289, at para 45. See also Loewenthal, "Article 291 TFEU" in Kellerbauer, Klamert and Tomkin, op. cit. *supra* note 69, pp. 1925–1932, at p. 1927.

162. Art. 97(1) GDPR.

163. Art. 97(2)(a) GDPR.

164. Art. 97(5) GDPR.

defined and the interaction between Article 3 and Chapter V be clarified in the GDPR when it is next reviewed.

6.5. *The role of the legislature*

The ECJ has stressed the importance of "clear and precise rules governing the scope and application of a measure" in the context of data transfers,[165] and legislation is the best way to produce such clarification in line with democratic accountability. A model in this regard is provided by the New Zealand Privacy Act 2020, which regulates the interaction of territorial scope and data transfer rules directly in legislation.[166]

The best way to deal with the interaction of territorial scope and data transfer rules, and to ensure that they work together to maximize the protection of data, would be to combine them in a single provision in the GDPR dealing with protection against external threats to EU data. This could be done in many different ways, which cannot be discussed further here. Inspiration for such revision could be drawn from the factors the EDPB has mentioned that need to be addressed when coordinating territorial scope and data transfer rules. For example, avoiding duplication of provisions resulting from the application of Article 3 and Chapter V; addressing protections that are missing through the application of Article 3 alone; and ensuring that the sole application of Article 3 does not result in a gap in enforcement as compared to Chapter V.[167]

Since data transfer rules provide for a greater possibility of enforcement than extraterritorial application of the GDPR under Article 3 does, and most data transfer mechanisms contain protections based on the GDPR, it would be best to provide that the GDPR does not apply to data processing that has been transferred subject to one of the data transfer mechanisms set out in Chapter V, rather than vice versa. In addition, including a definition of international data transfer in the GDPR that covers situations when individuals provide their own data to websites would enhance the effectiveness of protection by requiring parties that control such sites to be responsible for complying with Chapter V. It would also close the loophole that presently exists for EU individuals

165. Case C-362/14, *Schrems*, at para 91. See also Opinion 1/15, *EU-Canada PNR Agreement*, at para 141.

166. See New Zealand Privacy Act 2020, Public Act 2020 No. 31, available at <www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html>, Section 193 and Principle 12. See also New Zealand Privacy Commissioner, "New guidance for sending personal information overseas", available at <www.privacy.org.nz/publications/statements-media-releases/new-guidance-for-sending-personal-information-overseas/>.

167. EDPB Guidelines 5/2021 cited *supra* note 53, at 9.

entering their personal data onto non-EU websites by providing that any transfer of data to such sites must be carried out in accordance with Chapter V. Such measures would be an important step towards strengthening the EU's vision of protecting data processed and transferred outside its borders, and to interpret the protections contained in the GDPR consistently.